

First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities

Executive Summary

This document sets out an overview of the implementation and enforcement of the General Data Protection Regulation (GDPR) covering both the cooperation mechanism and the consistency findings.

In comparison with the EC Directive 95/46/EC, where Supervisory Authorities (SAs) were working separately even on cross-border cases, the GDPR created a duty for the SAs to cooperate in order to provide a consistent application of the GDPR. In addition to that, the European Data Protection Board (EDPB) provides a consistency mechanism to further foster the harmonisation.

Nine months after the entry into application of the GDPR, the members of the EDPB are of the opinion that the GDPR cooperation and consistency mechanism work quite well in practice. The national supervisory authorities make daily efforts to facilitate this cooperation, which implies numerous exchanges (written and oral) between them.

These cooperation duties lead to extra workloads, additional time dealing with cases and have an impact on the budget of the regulators. The handling of cross border cases takes time, due to the cooperation, to the need to carry out thorough investigations and in order to national procedural rules. The national SAs have to tackle these challenges regarding the harmonized protection and enforcement of the GDPR.

Until now, there are 6 final One-Stop-Shop cases.

The experiences of the EDPB regarding consistency is – up to now – limited, as no dispute resolution through this new EU body was necessary during the reported period.

I. Cooperation mechanism among SAs and the consistency mechanism of the EDPB

Cooperation mechanism

The GDPR requires close cooperation between SAs of EEA (EU-28 + Iceland, Norway and Liechtenstein) in cases implying a cross-border component and supports this by using the following tools:

- the mutual assistance,
- the joint operation,
- the One-Stop-Shop cooperation mechanism, which introduces the obligatory intervention of a Lead Supervisory Authority for the cross-border cases.

The cooperation on cross-border cases (ie. on the basis of complaints from individuals) is conducted by the national supervisory authorities. The EDPB does not deal with those cases unless a dispute arises between the authorities or in the case of urgency.

Consistency mechanism

One of the main tasks of the EDPB is to ensure the consistent application of the GDPR.

One opportunity to ensure consistency is to provide **general guidance** on the interpretation of the GDPR, which will contribute to a common understanding and application of the provisions by the stakeholders, the supervisory authorities and the public in general. Since 25 May 2018, the EDPB has endorsed 16 guidelines prepared by the Article 29 Working Party (predecessor of the EDPB) and has adopted 5 additional guidelines.

Another opportunity is to adopt **consistency opinions and decisions**. These decisions mainly address the national supervisory authorities and ensures a consistent application and enforcement of the GDPR.

Standardised communication:

To support the cooperation and the consistency mechanism among the EDPB members the DG Grow of the EU Commission, together with the EDPB Secretariat and the EDPB members, have customised an already existing IT system – the Internal Market Information system (IMI). This system was operational on the first day of the entry into application of the GDPR. This system provides a structured and confidential way to share information among the SAs.

The feedback of the national regulators on this system is really positive. A dedicated expert subgroup has been created to ensure the continuous enhancement of the system on the basis of the feedback collected via a dedicated IT Helpdesk support provided to the EDPB members by the EDPB Secretariat.

Before a case is produced in the case register of the system, the competent authorities have to be identified. This registry is the central database from which different procedures can be started, such as the mutual assistance, joint operation and One-Stop-Shop mechanism.

The scheme in the appendix provides an overview of the functioning of the system.

1. Cooperation Mechanism

a. Preliminary procedure to identify the lead and concerned supervisory authorities

Before starting a One-Stop-Shop procedure for cross-border cases, it is necessary to identify the authority that will lead the cooperation (Lead SA), and the other Concerned supervisory authorities (Concerned SA). The Lead SA will have to lead the cooperation procedure, draft the decision and the Concerned SAs will have the opportunity to raise objections.

The Lead SA is the authority within the EEA where the organisation subject to the investigation has its main establishment. The main establishment is identified as the central administration of the investigated company/organisation in the EU.

The EDPB created workflows in the IMI system to enable the SAs to identify their respective roles. The main purpose of this procedure is to define the roles at an early stage and to avoid objections on the question of competences at a later stage of the procedure.

In case of conflicting views regarding which authority should act as Lead SA, EDPB has the role of a dispute resolution body and issues a binding decision.

Since 25 May 2018, **642 procedures have been initiated to identify the Lead SA and the Concerned SAs** in cross-border cases. Out of the 642 procedures, **306 are closed and the Lead SA identified**.

Up to now, no dispute arose on the selection of the Lead SA.

24 EEA countries already initiated procedures and 26 SAs were proposed to act as lead SA.

b. Data base regarding cases with cross-border component

These cases will be registered in a central database from which different procedures can be initiated, such as the mutual assistance, joint operation and One-Stop-Shop mechanism.

Since 25 May 2018, 30 different EEA SAs have registered a total amount of **281 cases with cross-border component** in the IMI system.

The large part of the opened cases derived from **complaints by individuals (194 cases)**. The rest of the cases (87) has other origins.

The **three main topics** of the cases are related to the **exercise of the data subjects' rights, to the consumer rights and to data breaches**.

c. One-Stop-Shop Mechanism

The GDPR provides a specific cooperation procedure (One-Stop-Shop) for cross-border cases. A cross border case emerges where the controller or the processor has an establishment in more than one Member State or where the data processing activity substantially affects individuals in more than one Member State.

The One-Stop-Shop mechanism implies a cooperation between the Lead SA and the Concerned SA. The Lead SA will lead the cooperation procedure and plays a key role in the process to reach consensus between the Concerned SAs and to reach a coordinated decision with regard to a data controller or processor.

The Lead SA first has to investigate the case while observing its national procedural rules (eg. provide the right to be heard to the affected persons). During this investigation phase, it can gather information from another supervisory authority via mutual assistance or conduct joint investigation, where foreseen in the respective national law.

The IMI system also offers the opportunity for the Lead SA to launch – if necessary – an **informal communication with all the Concerned SAs** to collect information to prepare its draft decision.

Once the Lead SA has completed the investigation, **it prepares a draft decision and communicates it** to the Concerned SAs. These can object to the draft decision, which either leads to a revised draft decision or triggers the dispute resolving mechanism of the board.

If a dispute arose on the draft decision and no consensus is found, the consistency mechanism is triggered and the case is referred to the EDPB. The EDPB will then act as a dispute resolution body and issue a binding decision on the case. The Lead SA will have to adopt its **final decision** on the basis of the decision of the EDPB.

If the Concerned SAs do not object to the initial draft decision, or the revised one, they are deemed in agreement with the draft decision. So, the Lead SA can adopt **its final decision**.

The IMI system offers different procedures to handle the One-Stop-Shop cases:

1. Informal consultation procedures,
2. Draft decisions or revised decision submitted by the Lead SA to the Concerned SAs,
3. Final One-Stop-Shop decisions submitted to the Concerned SAs and to the EDPB.

Since 25 May 2018, **45 One-Stop-Shop procedures were initiated by SAs from 14 different EEA countries**. The 45 procedures are at different stages: **23 are at the informal consultation level, 16 are at draft decision level and 6 are final decisions**.

These first final One-Stop-Shop decisions relate to the exercise of the rights of individuals (such as the right to erasure), the appropriate legal basis for data processing and data breach notifications.

The limited number of **One-Stop-Shop procedures can be explained because** the circulation of the **draft decision is the result of the investigations** conducted by the Lead SA respecting national administrative procedural laws. The number of One-Stop-Shop procedures are **increasing steadily**.

d. Mutual assistance

The mutual assistance procedure allows each SAs to ask for information to other SAs but also to request any other measures for effective cooperation (such as prior authorisations, investigations, etc.).

The mutual assistance can be used for cross-border cases subject to the One-Stop-Shop procedure (as part of the preliminary phase to gather elements necessary before drafting a decision), or can also be used for national cases with cross-border component.

The IMI system enables the use of **informal mutual assistance**, **without any legal deadline** or the use of **formal mutual assistance** where the requested SA has **a legal deadline of 1 month** to reply to the request.

Since 25 May 2018, **444 mutual assistance requests (formal and informal)** have been triggered by **SAs from 18 different EEA countries**.

In 353 cases out of the 444 mutual assistance requests, **the answers were sent within 23 days**. The remaining 91 cases are ongoing, not yet answered by the requested SA.

e. Joint operations

The GDPR allows the SAs of different member states to carry out joint investigations and joint enforcement measures. The joint operations can be used in the context of cross-border cases subject to the One-Stop-Shop procedure (as part of the preliminary phase to gather elements necessary before the drafting a decision), or can also be used for national cases including a cross-border component.

Since 25 May 2018 to 31 January 2019, **no joint operations have been initiated**.

f. Assessment of the cooperation mechanism and suggestions for improvement by the SAs

In comparison with the EC Directive 95/46/EC where SAs were working separately even on cross border cases, the GDPR foresees a duty for the SAs to cooperate in order to provide a consistent application of the GDPR.

The national regulators adapted to this new situation. One of the advantages of the GDPR is to let some margin of manoeuvre for the SA to address those challenges.

However, the GDPR has been in application only for 9 months and there is still work to be done at the EDPB level to further streamline the procedure to make the system even more efficient. The question of the resources allocated to the authorities (and the possibility to recruit staff speaking also English) has impacts on the global efficiency of the system.

2. Consistency Mechanism

a. Consistency opinion

For some type of decisions, the national SAs have to require an opinion of the EDPB before being entitled to adopt its decision. This applies for instance to the approval of cross-border codes of conducts, the adoption of standardised contractual clauses, or the adoption of national lists describing the type of processing that must be subject to a Data Protection Impact Assessment.

The purpose of the consistency opinion issued by the EDPB is to guarantee the consistent application of the GDPR in cases where a competent SA wants to adopt those specific measures.

Each national SA, the Chair of the EDPB or the Commission can ask the EDPB to issue a consistency opinion on any matter of general application or producing effects in more than one Member State.

Since 25 May 2018, 28 opinions on the national lists of processing subject to a Data Protection Impact Assessment and 1 opinion on a draft administrative arrangement for the transfer of personal data between financial supervisory authorities (in the EEA and outside of the EEA) have been adopted by the EDPB. Currently there are 3 ongoing procedures which are related to binding corporate rules, to a draft standard contract between Controllers and Processors and to the interplay between the GDPR and the ePrivacy Directive, in particular as regards the competence of the national data protection supervisory authorities.

b. Dispute resolution

The EDPB intervenes as dispute resolution body and adopt binding decisions, in order to ensure the consistent application of the GDPR, in following cases:

- A dispute takes place within the One-Stop-Shop mechanism (a Concerned SA raises a relevant and reasoned objection which is not followed by the Lead SA);
- A disagreement takes place on the determination of the Lead SA;
- A SA does not request or does not follow a consistency opinion of the EDPB.

From 25 May 2018 to 18 February 2019, **no dispute resolutions were initiated**. This means that up to now, the SAs were able to reach consensus in all current cases, which is a good sign in terms of cooperation.

c. Assessment of the consistency mechanism and suggestion for improvement by the SAs

The following analysis reflects the views and impressions of the authorities in the context of this report.

Up to now, the EDPB did not have to act as a dispute resolution body, also due to the fact that the number of decisions resulting from the One-Stop-Shop cases is still relatively small.

Since the EDPB has so far focused mainly on the preparation of consistency opinions on national DPIA lists (on the national lists of processing subject to a Data Protection Impact Assessment) most authorities emphasised that the experience of the EDPB with the consistency mechanism in other areas is still limited. However, it is planned that in the coming months other types of national measures, such as BCRs, codes of conducts, standard contracts and issues related to certification will be submitted to the EDPB and thus trigger the consistency mechanism in other fields.

It was indicated that, already on the basis of the first experiences the consistency mechanisms was found to require many resources, to be time-consuming and to require the authorities to act swiftly within the given timeframe. In this context, a possible need to extend the deadlines was addressed.

II. Means and powers of the national supervisory authorities

1. Budget and human resources

Under the new legal framework, SAs wear two hats. They not only deal with their enhanced enforcement powers but are required to become more engaged, which implies the need for more budget and staff.

a. Budget

While, based on information provided by SAs from 26 EEA countries and the EDPS, in most cases an increase in the budget for 2018 and 2019 was observed, in two cases a decrease and in 3 cases no changes in the budget were noticed. According to information provided by the respective SAs, the latter phenomena can be explained by biannual plans for this period of time.

Although the majority of the 17 replying SAs stated that they would need an increase in the budget of 30-50%, almost none of them received the requested amount. There are some extreme examples where this need is close to or even 100 %.

b. Human resources

Based on information provided by SAs from 26 EEA countries and the EDPS, the majority of SAs have experienced an increase in the number of staff, while for 8 SAs the human resources did not change. For one SA, there was even a decrease in personnel.

Given the different scope of competences of the SAs (GDPR, e-Privacy, Freedom of Information), the requirements for more personnel also vary.

2. Implementation and enforcement of the GDPR at national level

The total number of cases reported by SAs from 31 EEA countries is 206.326. Three different types of the cases can be distinguished, namely cases based on complaints, cases based on data breach notifications and other types of cases. The majority of the cases are related to complaints, notably 94.622 while 64.684 were initiated on the basis of data breach notification by the controller.

52 % of these cases have already been closed and 1 % of these cases challenged before national court.

Corrective powers:

Regarding the corrective powers, the SAs have different measures to use:

- to issue warnings to a controller or processor that intended processing operations are likely to infringe the GDPR,
- to issue reprimands to a controller or a processor where processing operations have infringed the GDPR,
- to order the controller or the processor to comply with the data subject's requests or to bring processing operations into compliance with the GDPR,
- to impose administrative limitations, bans and fines.

SAs from 11 EEA countries have already imposed administrative fines according to Article 58.2

(i) GDPR. The total amount of the imposed fine is 55.955.871 EUR.

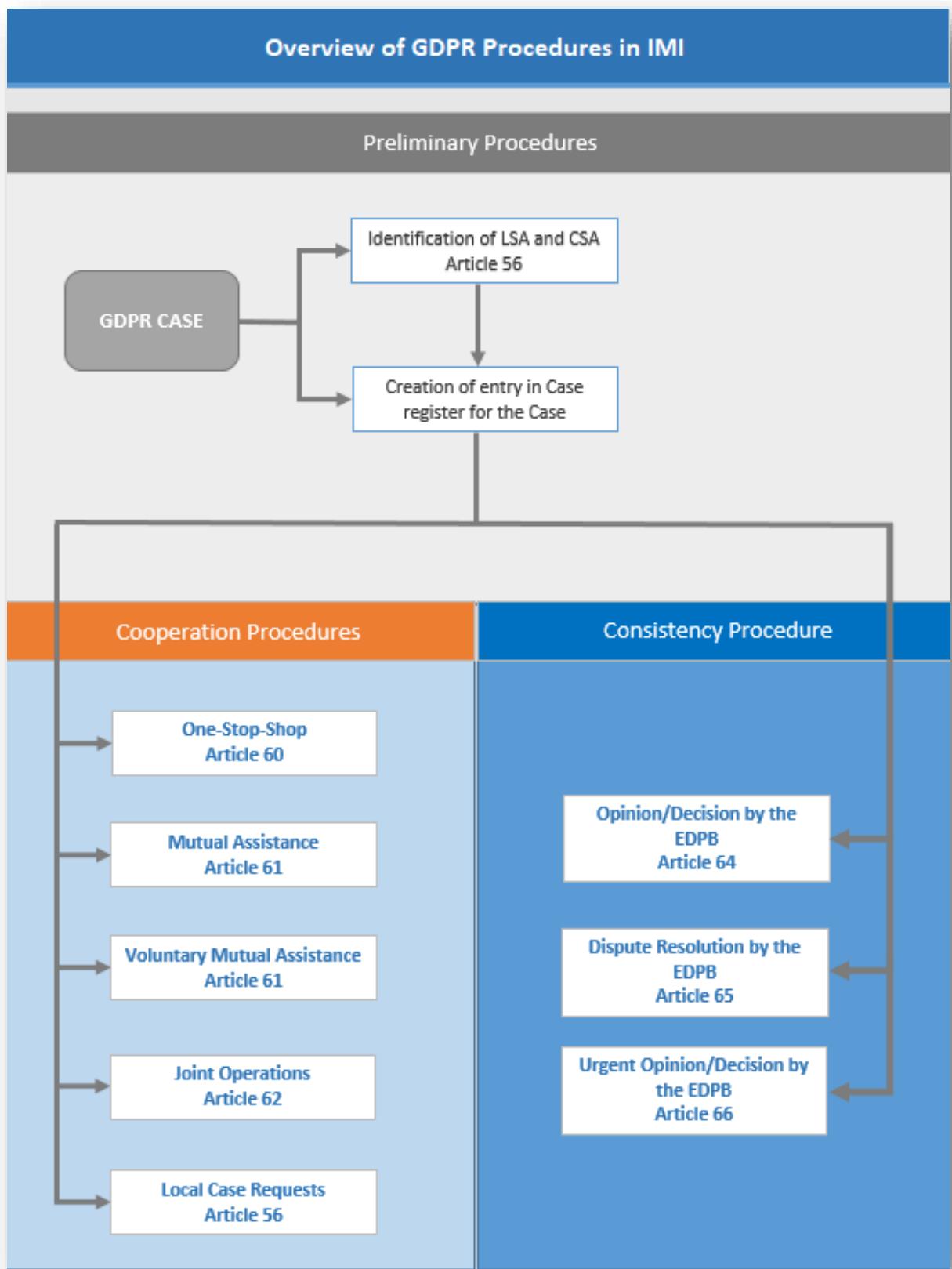
III. Conclusion

Nine months after the entry into application of the GDPR, the members of the EDPB are of the opinion that the GDPR works quite well in practice making use of the new way of cooperation including numerous daily exchanges. The One-Stop-Shop cases that have already led to an outcome tested some of the core principles of the GDPR and were resolved smoothly. So far, not a single cross-border case has been escalated to the EDPB level.

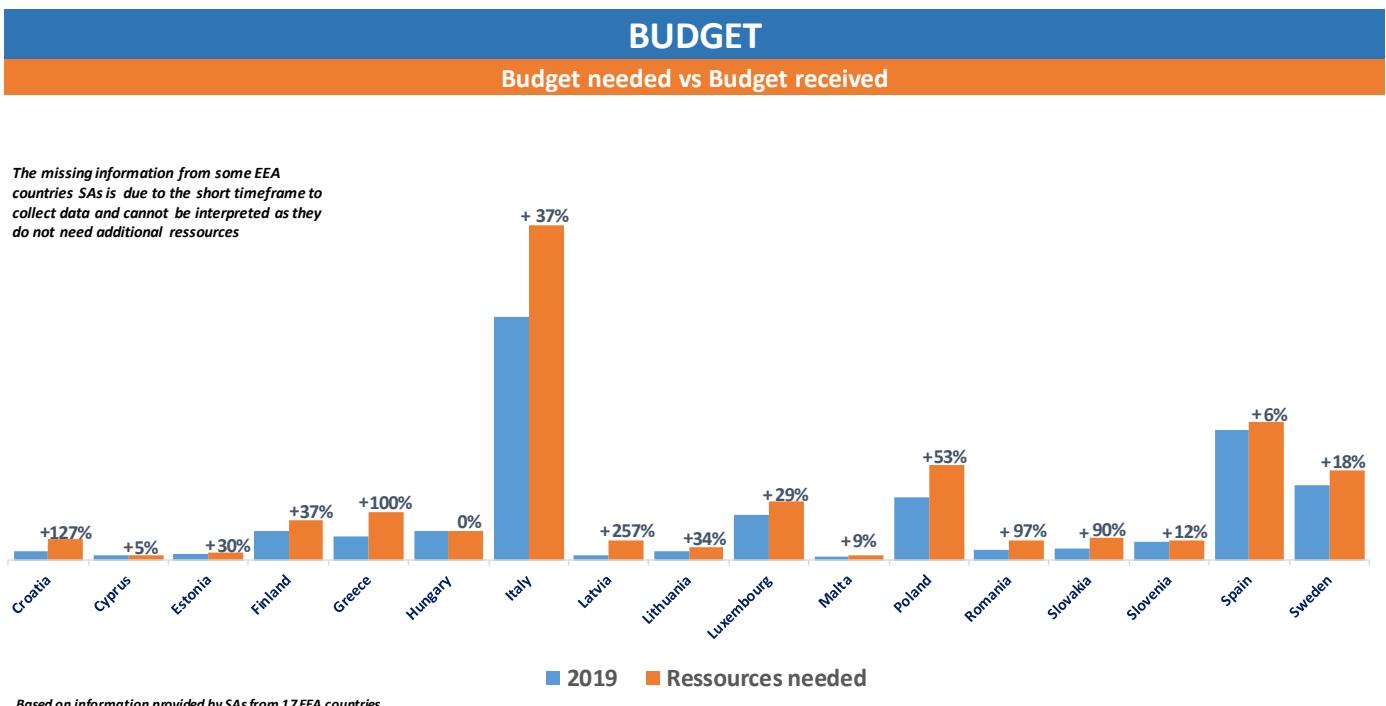
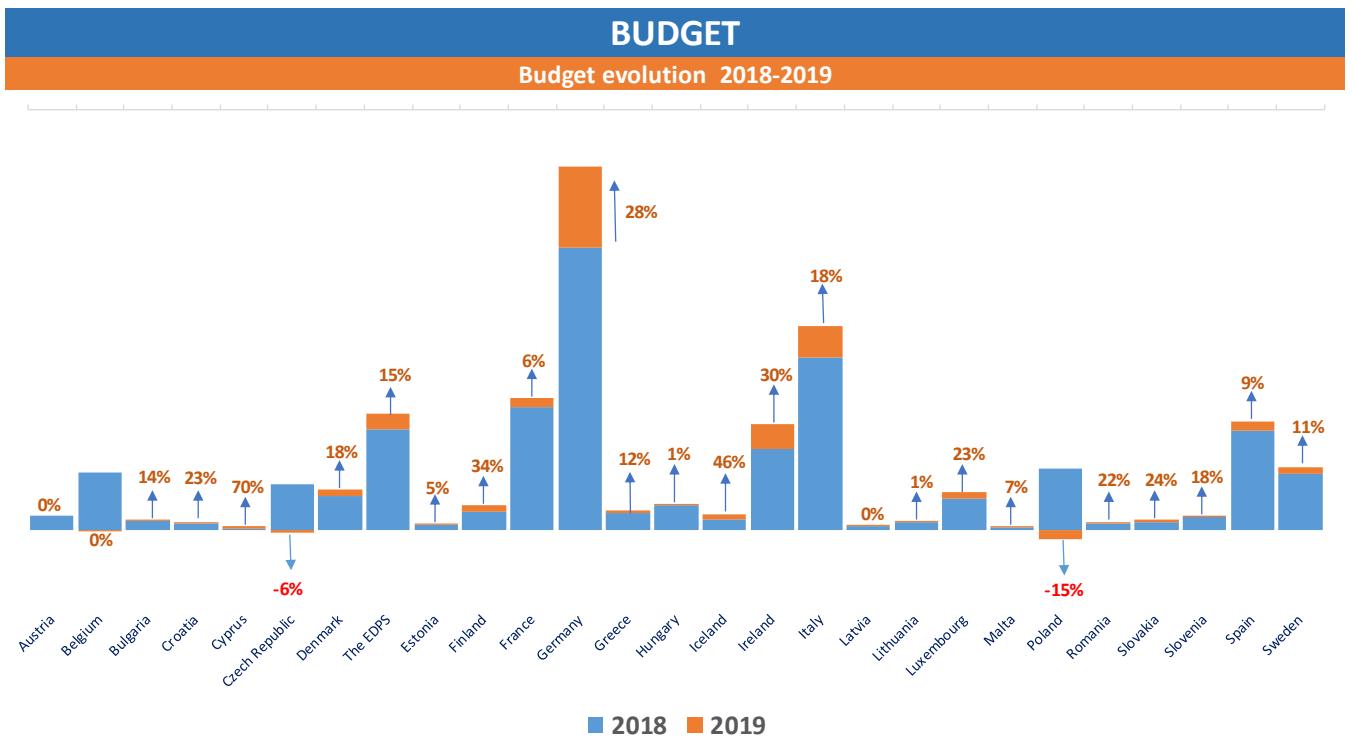
Despite the increase in the number of cases in the last months, the SAs reported that the workload is manageable for the moment, in large part thanks to a thorough preparation during the past two years by SAs, the Article 29 Working Party and by the Board.

Appendix

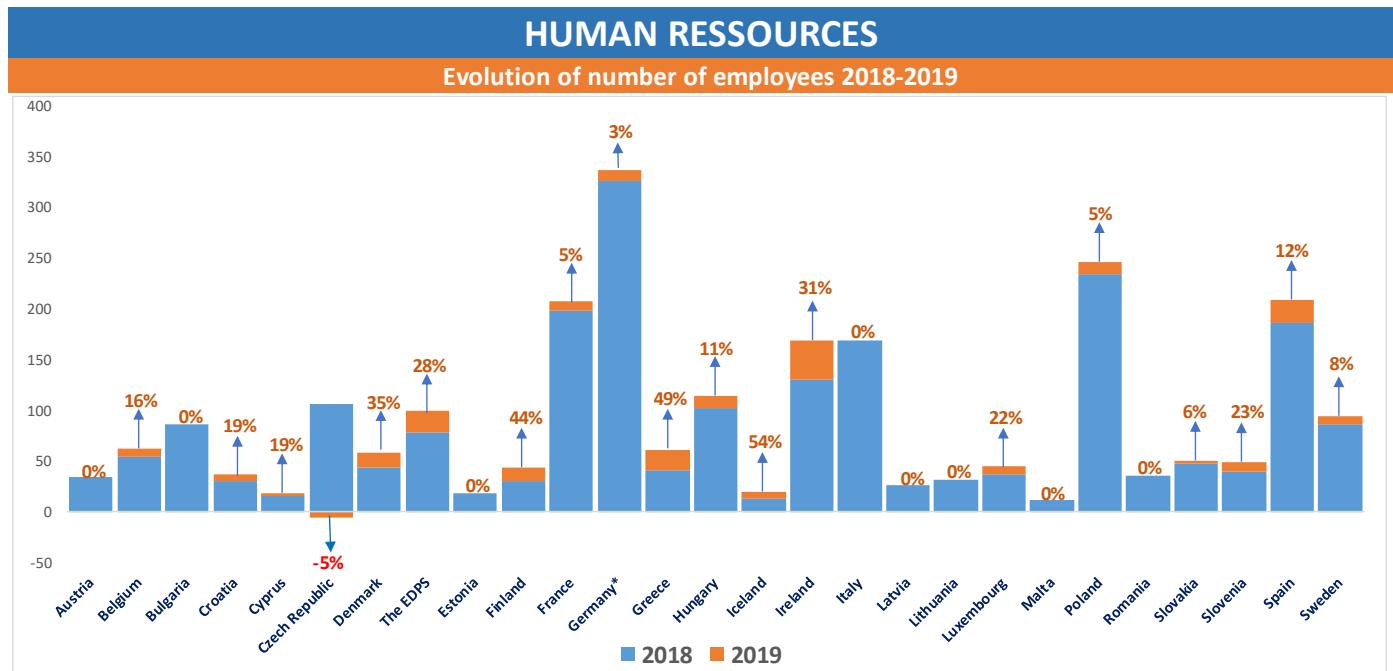
Cooperation mechanism among SAs and the consistency mechanism of the EDPB



Budget

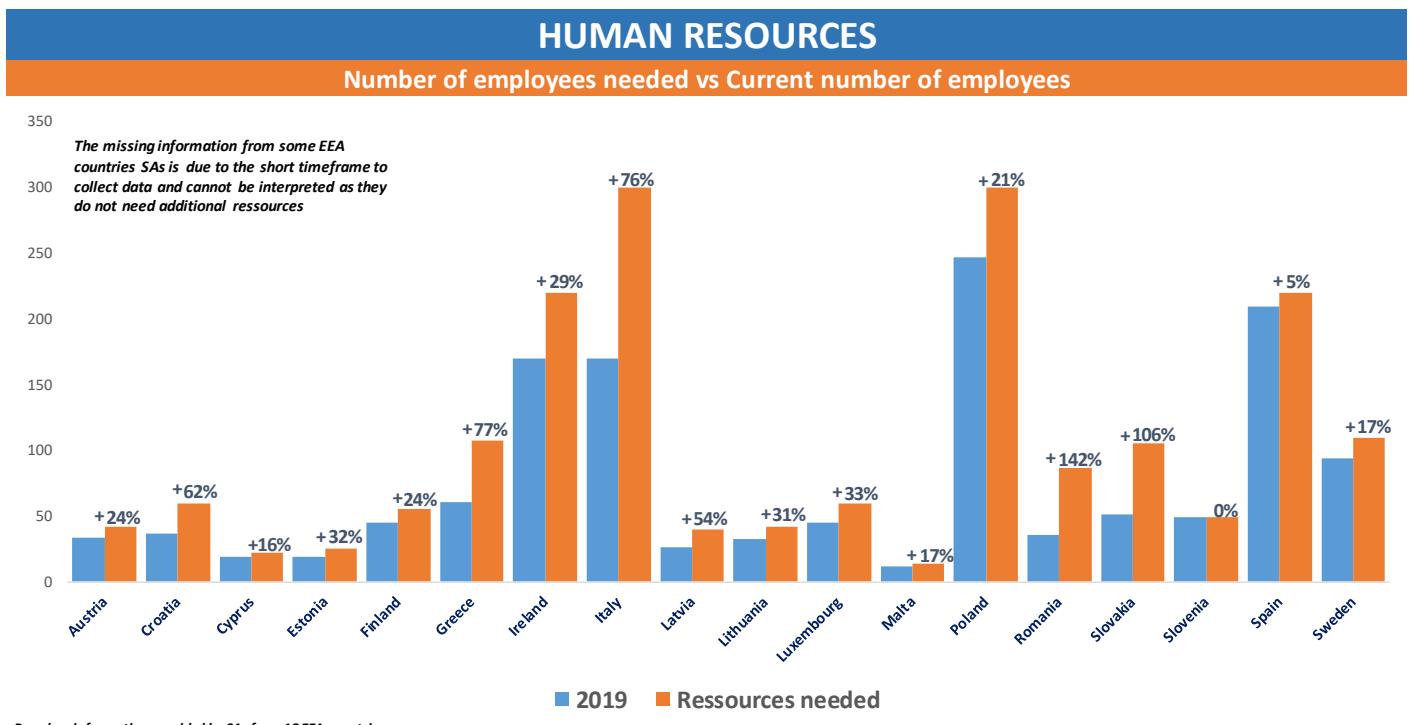


Human resources



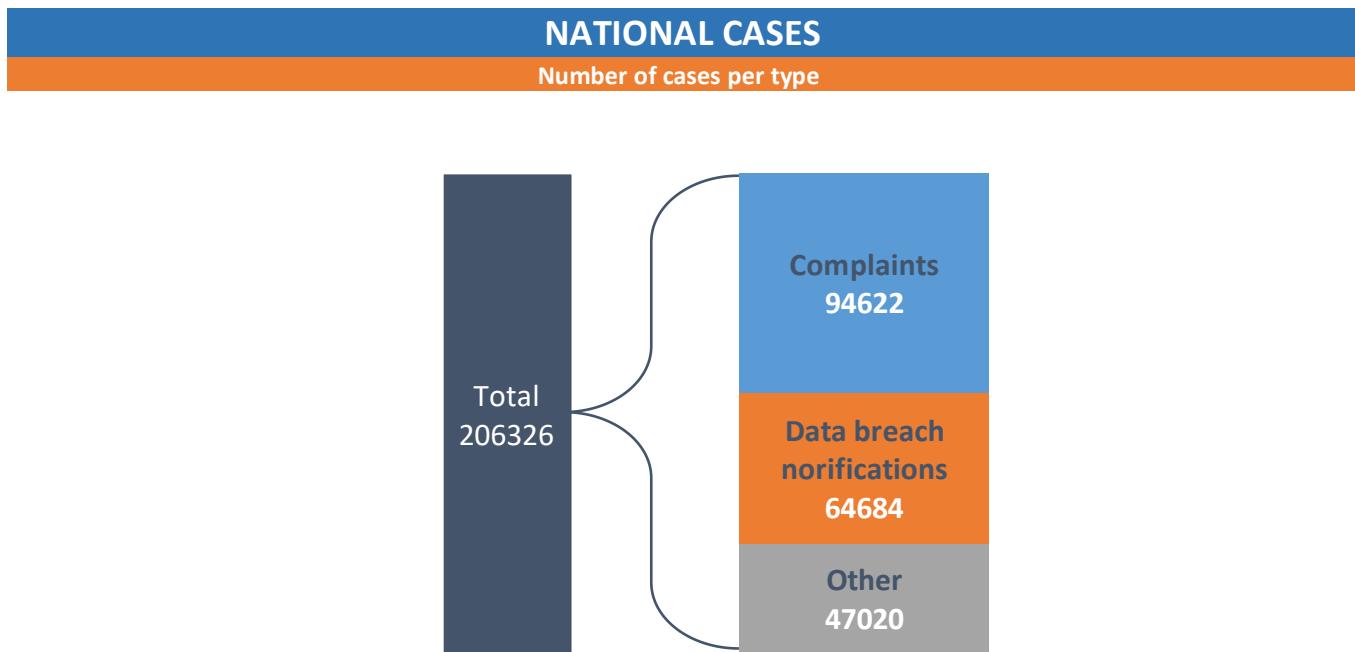
Based on information provided by SAs from 26 EEA countries and the EDPS

* Germany: Based on information provided by 9 Regional SAs



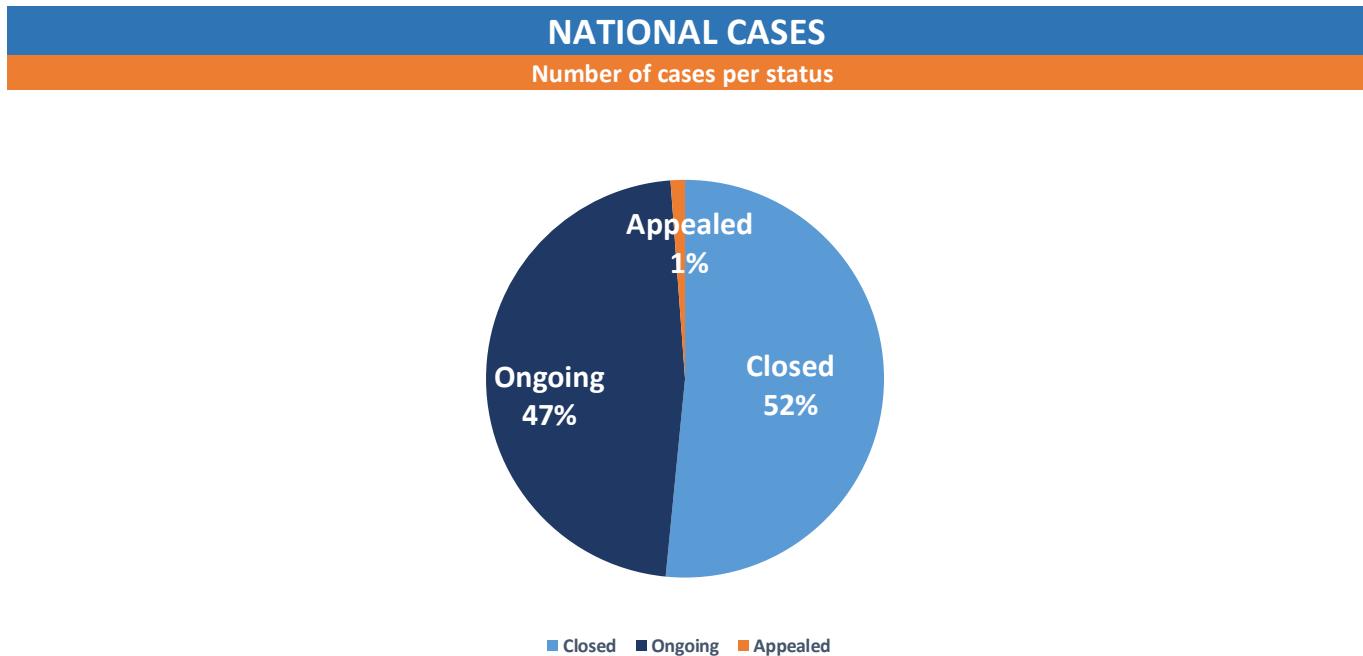
Based on information provided by SAs from 18 EEA countries

Implementation and enforcement of the GDPR at national level



Based on information provided by SAs from 31 EEA countries

*Germany: Based on information provided by The Federal and 13 Regional SAs



Based on information provided by SAs from 23 EEA countries (Case status information provided for 72883 cases)

*Germany: Based on information provided by The Federal and 5 Regional SAs

FINES

Number of imposed fines



SAs from **11** EEA countries imposed a total of **€55,955,871** fine

Based on information provided by SAs from 11 EEA countries

Germany: Based on information provided by 4 regional SAs

Opinion of the Board (Art. 64)



Opinion 1/2018

on the draft list of the competent supervisory authority of Austria

regarding

**the processing operations subject to the requirement of a data protection
impact assessment (Article 35.4 GDPR)**

Adopted on 25th September 2018

Contents

1.	Summary of the Facts	4
2.	Assessment	5
2.1	General reasoning of the EDPB regarding the submitted list	5
2.2	Application of the consistency mechanism to the draft list	6
2.3	Analysis of the draft list.....	6
	Indicative nature of the list.....	6
	Reference to the Guidelines	6
	Biometric data.....	6
	Genetic data.....	6
	Data collected via third parties (article 19 GDPR)	7
	Joint Controllership.....	7
	Processing using new/innovative technology	7
3.	Conclusions / Recommendations	7
4.	Final Remarks	8

The European Data Protection Board

Having regard to Article 63, Article 64 (1a), (3) - (8) and Article 35 (1), (3), (4), (6) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (here after GDPR) throughout the European Economic Area. In compliance with article 64.1 GDPR, the Board has to issue an opinion where a supervisory authority intends to adopt a list of processing operations subject to the requirement for a data protection impact assessment pursuant to article 35.4 GDPR. The aim of this opinion is therefore to create a harmonized approach with regard to processing that is cross border or that can affect the free flow of personal data or natural person across the European Union. Even though the GDPR doesn't impose a single list, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by requesting SAs to include some types of processing in their lists, secondly by requesting them to remove some criteria which the Board doesn't consider as necessarily creating high risks for data subjects, and finally by requesting them to use some criteria in a harmonized manner.

(2) With reference to Article 35 (4) and (6)GDPR, the competent supervisory authorities shall establish lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment (hereinafter "DPIA"). They shall, however, apply the consistency mechanism where such lists involve processing operations, which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

(3) While the draft lists of the competent supervisory authorities are subject to the consistency mechanism, this does not mean that the lists should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB assessment/opinion is not to reach a single EU list but rather to avoid significant inconsistencies that may affect the equivalent protection of the data subjects.

(4) The carrying out of a DPIA is only mandatory for the controller pursuant to Article 35 (1) GDPR where processing is "likely to result in a high risk to the rights and freedoms of natural

persons". Article 35 (3) GDPR illustrates what is likely to result in a high risk. This is a non-exhaustive list. The Working Party 29 in the Guidelines on data protection impact assessment¹, as endorsed by the EDPB², has clarified criteria that can help to identify when processing operations are subject to the requirement for a DPIA. The Working Party 29 Guidelines WP248 state that in most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out, however, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

(5) The lists produced by the competent supervisory authorities support the same objective to identify processing operations likely to result in a high risk and processing operations which therefore require a DPIA. As such, the criteria developed in the Working Party 29 Guidelines should be applied when assessing whether the draft lists of the competent supervisory authorities does not affect the consistent application of the GDPR.

(6) Twenty-two competent supervisory authorities have submitted their draft lists to the EDPB. A global assessment of these draft lists supports the objective of a consistent application of the GDPR even though the complexity of the subject matter increases.

(7) The opinion of the EDPB shall be adopted pursuant to Article 64 (3) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

I. Summary of the Facts

The competent supervisory authority of Austria has submitted its draft list to the EDPB. The decision on the completeness of the file was taken on 10th July 2018. The period until which the opinion has to be adopted has been extended until the 25th of September taking into account the complexity of the subject matter considering that at the same time twenty-two competent supervisory authorities submitted the draft lists and thus the need for a global assessment arose.

¹ WP29, Guidelines on Data Protection Impact Assessment and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP 248 rev. 01).

² EDPB, Endorsement 1/2018.

2. Assessment

2.1 General reasoning of the EDPB regarding the submitted list

Any list submitted to the EDPB has been interpreted as further specifying Art 35.1, which will prevail in any case. Thus, no list can be exhaustive. As the list provided by Österreichische Datenschutzbehörde (hereafter Austrian Supervisory Authority) does not explicitly state this, the Board requests this explanation to be added to the document containing the list.

In compliance with article 35.10 GDPR, the Board is of the opinion that if a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of the legal basis the obligation to carry out a DPIA in accordance with paragraphs 1 to 7 of article 35 GDPR does not apply, unless the Member State deems it necessary.

Further, if the Board requests a DPIA for a certain category of processing and an equivalent measure is already required by national law, the Austrian Supervisory Authority shall add a reference to this measure.

This opinion does not reflect upon items submitted by the Austrian Supervisory Authority, which were deemed outside the scope of Article 35.6 GDPR. This refers to items that neither relate “to the offering of goods or services to data subjects” in several Member States nor to the monitoring of the behaviour of data subjects in several Member States. Additionally, they are not likely to “substantially affect the free movement of personal data within the Union”. This is especially the case for items relating to national legislation and in particular where the obligation to carry out a DPIA is stipulated in national legislation. Further, any processing operations that relate to law enforcement were deemed out of scope, as they are not in scope of the GDPR.

The Board has noted that several supervisory authorities have included in their lists some types of processing which are necessarily local processing. Given that only cross border processing and processing that may affect the free flow of personal data and data subjects are concerned by Article 35.6, the Board will not comment on those local processing.

The opinion aims at defining a consistent core of processing operations that are recurrent in the lists provided by the SAs.

This means that, for a limited number of types of processing operations, that will be defined in a harmonised way, all the Supervisory Authorities will require a DPIA to be carried out and the Board will recommend the SAs to amend their lists accordingly in order to ensure consistency.

When this opinion remains silent on DPIA list entries submitted, it means that the Board is not asking the Austrian Supervisory Authority to take further action.

Finally, the Board recalls that transparency is key for data controllers and data processors. In order to clarify the entries in the list, the Board is of the opinion that making an explicit reference in the lists, for each type of processing, to the criteria set out in the guidelines could

improve this transparency. Therefore, the Board considers that an explanation on which criteria have been taken into account by the Austrian Supervisory Authority to create its list could be added.

2.2 Application of the consistency mechanism to the draft list

The draft list submitted by the Austrian Supervisory Authority relates to the offering of goods or services to data subjects, relates to the monitoring of their behaviour in several Member States and/or may substantially affect the free movement of personal data within the Union mainly because the processing operations in the submitted draft list are not limited to data subjects in this country.

2.3 Analysis of the draft list

Taking into account that:

- a. Article 35 (1) GDPR requires a DPIA when the processing activity is likely to result in a high risk to the rights and freedoms of natural persons; and
- b. Article 35 (3) GDPR provides a non-exhaustive list of types of processing that require a DPIA,

the Board is of the opinion that:

INDICATIVE NATURE OF THE LIST

As the list provided by Austrian Supervisory Authority does not explicitly state that its list is not exhaustive, the Board requests this explanation to be added to the document containing the list.

REFERENCE TO THE GUIDELINES

The board is of the opinion that the analysis done in the Working Party 29 Guidelines WP248 are a core element for ensuring consistency across the Union. Thus, it requests the different Supervisor Authorities to add a statement to the document containing their list that clarifies that their list is based on these guidelines and that it complements and further specifies the guidelines.

As the document of the Austrian Supervisory Authority does not contain such a statement, the Board recommends the Austrian Supervisory Authority to amend its document accordingly.

BIOMETRIC DATA

The list submitted by the Austrian Supervisory Authority for an opinion of the Board envisages that the processing of biometric data for the purpose of uniquely identifying a natural person, in conjunction with at least one other criterion, requires a DPIA. On this point, the Board acknowledges that the list aligns with the aim of consistency.

GENETIC DATA

The list submitted by the Austrian Supervisory Authority for an opinion of the Board envisages that the processing of genetic data, in conjunction with at least one other criterion, requires

a DPIA. The Board is of the opinion that the processing of genetic data on its own is not necessarily likely to represent a high risk. However, the processing of genetic data in conjunction with at least one other criterion requires a DPIA to be carried out. The Board takes note of the inclusion of this criterion in the list of Austrian Supervisory Authority.

DATA COLLECTED VIA THIRD PARTIES (ARTICLE 19 GDPR)

The Board is of the opinion that types of processing activities that could deprive the data subjects from their rights on their own do not represent a high risk. Further, the Board is of the opinion that a processing activity conducted by the controller under article 19 GDPR and where the information of recipients would prove impossible or require a disproportionate effort only requires a DPIA to be carried out when this processing involves at least one other criterion. The list submitted by the Austrian Supervisory Authority for an opinion of the Board states that this type of processing on its own falls under the obligation to perform a DPIA. The Board requests the Austrian Supervisory Authority to amend its list accordingly, by adding to the item contained in § 2, (2), 6 of its list which references the processing of personal data collected via third parties that it requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.

JOINT CONTROLLERSHIP

The Board is of the opinion that joint controllership should not be a criterion leading to an obligation to do a DPIA, alone or with another criterion. Thus, the processing of personal data under a joint controllership should not per se require a DPIA to be carried out. The list submitted by the Austrian Supervisory Authority for an opinion of the Board does currently require a DPIA to be carried out when there is a processing under a joint controllership. The Board requests the Austrian Supervisory Authority to amend its list accordingly, by removing the item of processing under a joint controllership from its list.

PROCESSING USING NEW/INNOVATIVE TECHNOLOGY

The list submitted by the Austrian Supervisory Authority for an opinion of the Board envisages that the processing of personal data using innovative technology in conjunction with at least one other criterion, requires a DPIA. The Board takes note of the inclusion of this criterion in the list.

3. Conclusions / Recommendations

The draft list of the Austrian Supervisory Authority may lead to an inconsistent application of the requirement for a DPIA and the following changes need to be made:

- Regarding the indicative nature of the list: the Board requests an explanation to be added to the document containing the list, stating its non-exhaustive nature.
- Regarding the reference to the guidelines: the Board requests the Austrian Supervisory Authority to amend its document accordingly.
- Regarding data collected via third parties (article 19 GDPR): the Board requests the Austrian Supervisory Authority to amend its list by adding that the item referencing

the processing of personal data collected via third parties requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.

- Regarding joint controllership: the Board requests the Austrian Supervisory Authority to amend its list by removing the reference to joint controllership from its list.

4. Final Remarks

This opinion is addressed to the Österreichische Datenschutzbehörde (Austrian Supervisory Authority) and will be made public pursuant to Article 64 (5b) GDPR.

According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 2/2018

on the draft list of the competent supervisory authority of Belgium

regarding

**the processing operations subject to the requirement of a data protection
impact assessment (Article 35.4 GDPR)**

Adopted on 25th September 2018

Contents

1.	Summary of the Facts	4
2.	Assessment	5
2.1	General reasoning of the EDPB regarding the submitted list	5
2.2	Application of the consistency mechanism to the draft list	6
2.3	Analysis of the draft list.....	6
	Reference to the Guidelines	6
	Biometric data.....	6
	Genetic data.....	6
	Data collected via third parties (article 19 GDPR)	7
	Employee monitoring	7
	Processing carried out with the aid of an implant.....	7
	Processing using new/innovative technology	7
3.	Conclusions / Recommendations	7
4.	Final Remarks	8

The European Data Protection Board

Having regard to Article 63, Article 64 (1a), (3) - (8) and Article 35 (1), (3), (4), (6) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (here after GDPR) throughout the European Economic Area. In compliance with article 64.1 GDPR, the Board has to issue an opinion where a supervisory authority intends to adopt a list of processing operations subject to the requirement for a data protection impact assessment pursuant to article 35.4 GDPR. The aim of this opinion is therefore to create a harmonized approach with regard to processing that is cross border or that can affect the free flow of personal data or natural person across the European Union. Even though the GDPR doesn't impose a single list, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by requesting SAs to include some types of processing in their lists, secondly by requesting them to remove some criteria which the Board doesn't consider as necessarily creating high risks for data subjects, and finally by requesting them to use some criteria in a harmonized manner.

(2) With reference to Article 35 (4) and (6)GDPR, the competent supervisory authorities shall establish lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment (hereinafter "DPIA"). They shall, however, apply the consistency mechanism where such lists involve processing operations, which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

(3) While the draft lists of the competent supervisory authorities are subject to the consistency mechanism, this does not mean that the lists should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB assessment/opinion is not to reach a single EU list but rather to avoid significant inconsistencies that may affect the equivalent protection of the data subjects.

(4) The carrying out of a DPIA is only mandatory for the controller pursuant to Article 35 (1) GDPR where processing is "likely to result in a high risk to the rights and freedoms of natural

persons". Article 35 (3) GDPR illustrates what is likely to result in a high risk. This is a non-exhaustive list. The Working Party 29 in the Guidelines on data protection impact assessment¹, as endorsed by the EDPB², has clarified criteria that can help to identify when processing operations are subject to the requirement for a DPIA. The Working Party 29 Guidelines WP248 state that in most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out, however, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

(5) The lists produced by the competent supervisory authorities support the same objective to identify processing operations likely to result in a high risk and processing operations, which therefore require a DPIA. As such, the criteria developed in the Working Party 29 Guidelines should be applied when assessing whether the draft lists of the competent supervisory authorities does not affect the consistent application of the GDPR.

(6) Twenty-two competent supervisory authorities have submitted their draft lists to the EDPB. A global assessment of these draft lists supports the objective of a consistent application of the GDPR even though the complexity of the subject matter increases.

(7) The opinion of the EDPB shall be adopted pursuant to Article 64 (3) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

I. Summary of the Facts

The Autorité de la protection des données (APD-GBA) (hereafter Belgian Supervisory Authority) has submitted its draft list to the EDPB. The decision on the completeness of the file was taken on 26th of June 2018. This period until which the opinion to be adopted has been extended until the 25th of September taking into account the complexity of the subject matter considering that at the same time twenty-two competent supervisory authorities submitted the draft lists and thus the need for a global assessment arose.

¹ WP29, Guidelines on Data Protection Impact Assessment and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP 248 rev. 01).

² EDPB, Endorsement 1/2018.

2. Assessment

2.1 General reasoning of the EDPB regarding the submitted list

Any list submitted to the EDPB has been interpreted as further specifying Art 35.1, which will prevail in any case. Thus, no list can be exhaustive.

In compliance with article 35.10 GDPR, the Board is of the opinion that if a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of the legal basis the obligation to carry out a DPIA in accordance with paragraphs 1 to 7 of article 35 GDPR does not apply, unless the Member State deems it necessary.

Further, if the Board requests a DPIA for a certain category of processing and an equivalent measure is already required by national law, the Belgian Supervisory Authority shall add a reference to this measure.

This opinion does not reflect upon items submitted by the Belgian Supervisory Authority, which were deemed outside the scope of Article 35.6 GDPR. This refers to items that neither relate “to the offering of goods or services to data subjects” in several Member States nor to the monitoring of the behaviour of data subjects in several Member States. Additionally, they are not likely to “substantially affect the free movement of personal data within the Union”. This is especially the case for items relating to national legislation and in particular where the obligation to carry out a DPIA is stipulated in national legislation. Further, any processing operations that relate to law enforcement were deemed out of scope, as they are not in scope of the GDPR.

The Board has noted that several supervisory authorities have included in their lists some types of processing which are necessarily local processing. Given that only cross border processing and processing that may affect the free flow of personal data and data subjects are concerned by Article 35.6, the Board will not comment on those local processing.

The opinion aims at defining a consistent core of processing operations that are recurrent in the lists provided by the SAs.

This means that, for a limited number of types of processing operations, that will be defined in a harmonised way, all the Supervisory Authorities will require a DPIA to be carried out and the Board will recommend the SAs to amend their lists accordingly in order to ensure consistency.

When this opinion remains silent on DPIA list entries submitted, it means that the Board is not asking the Belgian Supervisory Authority to take further action.

Finally, the Board recalls that transparency is key for data controllers and data processors. In order to clarify the entries in the list, the Board is of the opinion that making an explicit reference in the lists, for each type of processing, to the criteria set out in the guidelines could improve this transparency. Therefore, the Board considers that an explanation on which

criteria have been taken into account by the Belgian Supervisory Authority to create its list could be added.

2.2 Application of the consistency mechanism to the draft list

The submitted draft list by the Belgian Supervisory Authority relates to the offering of goods or services to data subjects, relates to the monitoring of their behaviour in several Member States and/or may substantially affect the free movement of personal data within the Union mainly because the processing operations in the submitted draft list are not limited to data subjects in this country.

2.3 Analysis of the draft list

Taking into account that:

- a. Article 35 (1) GDPR requires a DPIA when the processing activity is likely to result in a high risk to the rights and freedoms of natural persons; and
- b. Article 35 (3) GDPR provides a non-exhaustive list of types of processing that require a DPIA,

the Board is of the opinion that:

REFERENCE TO THE GUIDELINES

The board is of the opinion that the analysis done in the Working Party 29 Guidelines WP248 are a core element for ensuring consistency across the Union. Thus, it requests the different Supervisor Authorities to add a statement to the document containing their list that clarifies that their list is based on these guidelines and that it complements and further specifies the guidelines.

As the document of the Belgian Supervisory Authority does not contain such a statement, the Board recommends the Belgian Supervisory Authority to amend its document accordingly.

BIOMETRIC DATA

The list submitted by the Belgian Supervisory Authority for an opinion of the Board envisages that the processing of biometric data for the purpose of uniquely identifying a natural person, in conjunction with at least one other criterion, requires a DPIA. On this point, the Board acknowledges that the list aligns with the aim of consistency.

GENETIC DATA

The list submitted by the Belgian Supervisory Authority for an opinion of the Board envisages that the processing of genetic data, in conjunction with at least one other criterion, requires a DPIA. The Board is of the opinion that the processing of genetic data on its own is not necessarily likely to represent a high risk. However, the processing of genetic data in conjunction with at least one other criterion requires a DPIA to be carried out. The Board takes note of the inclusion of this criterion in the list of Belgian Supervisory Authority.

DATA COLLECTED VIA THIRD PARTIES (ARTICLE 19 GDPR)

The Board is of the opinion that types of processing activities that could deprive the data subjects from their rights in conjunction with at least one other criterion represent a high risk. Further, the Board is of the opinion that a processing activity conducted by the controller under article 19 GDPR and where the information of recipients would prove impossible or require a disproportionate effort only requires a DPIA to be carried out when this processing involves at least one other criterion. The list submitted by the Belgian Supervisory Authority for an opinion of the Board states that this type of processing in conjunction with at least one other criterion falls under the obligation to perform a DPIA. The Board takes note of the inclusion of this criterion in the list.

EMPLOYEE MONITORING

The Board is of the opinion that, due to its specific nature, the employee monitoring processing, meeting the criterion of vulnerable data subjects and of systematic monitoring in the guidelines, – could require a DPIA. Given that the list submitted by the Belgian Supervisory Authority for an opinion of the Board already envisages this type of processing as requiring a data protection impact assessment, the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248. In addition, the Board is of the opinion that the WP249 of the Article 29 working party remains valid when defining the concept of the systematic processing of employee data.

PROCESSING CARRIED OUT WITH THE AID OF AN IMPLANT

The Board is of the opinion that, the processing of non-health data with the aid of an implant does not require a DPIA in every instance. The list submitted by the Belgian Supervisory Authority for an opinion of the Board does currently not clarify that a DPIA is to be done for the processing of health data with the aid of an implant. As such, the Board requests the Belgian Supervisory Authority to amend its list accordingly, by stating that in any event the processing of health data with the aid of an implant requires a DPIA to be carried out.

PROCESSING USING NEW/INNOVATIVE TECHNOLOGY

The list submitted by the Belgian Supervisory Authority for an opinion of the Board envisages that the processing of personal data using innovative technology in conjunction with at least one other criterion, requires a DPIA. The Board takes note of the inclusion of this criterion in the list.

3. Conclusions / Recommendations

The draft list of the Belgian Supervisory Authority may lead to an inconsistent application of the requirement for a DPIA and the following changes need to made:

- Regarding the reference to the guidelines: the Board requests the Belgian Supervisory Authority to amend its document accordingly.
- Regarding employment monitoring: the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248.

- Regarding processing carried out with the aid of an implant: the Board requests the Belgian Supervisory Authority to amend its list by stating that only the processing of health data with the aid of an implant requires a DPIA to be carried out.

4. Final Remarks

This opinion is addressed to the Autorité de la protection des données (APD-GBA) (Belgian Supervisory Authority) and will be made public pursuant to Article 64 (5b) GDPR.

According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 3/2018

on the draft list of the competent supervisory authority of Bulgaria

regarding

**the processing operations subject to the requirement of a data protection
impact assessment (Article 35.4 GDPR)**

Adopted on 25th September 2018

Contents

1.	Summary of the Facts	4
2.	Assessment	5
2.1	General reasoning of the EDPB regarding the submitted list	5
2.2	Application of the consistency mechanism to the draft list	6
2.3	Analysis of the draft list.....	6
	Indicative nature of the list.....	6
	Reference to the Guidelines	6
	Biometric data.....	6
	Genetic data.....	7
	Biometric 'and' genetic data.....	7
	Location data	7
	Exceptions to information to be provided to the data subject according to Article 14.5 GDPR	7
	Referencing a specific legal basis.....	7
	Joint Controllership.....	8
	Territorially-distributed or cross-border information systems	8
	Migration from one system to at least one other	8
	Processing using new/innovative technology	8
3.	Conclusions / Recommendations	8
4.	Final Remarks	9

The European Data Protection Board

Having regard to Article 63, Article 64 (1a), (3) - (8) and Article 35 (1), (3), (4), (6) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (here after GDPR) throughout the European Economic Area. In compliance with article 64.1 GDPR, the Board has to issue an opinion where a supervisory authority intends to adopt a list of processing operations subject to the requirement for a data protection impact assessment pursuant to article 35.4 GDPR. The aim of this opinion is therefore to create a harmonized approach with regard to processing that is cross border or that can affect the free flow of personal data or natural person across the European Union. Even though the GDPR doesn't impose a single list, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by requesting SAs to include some types of processing in their lists, secondly by requesting them to remove some criteria which the Board doesn't consider as necessarily creating high risks for data subjects, and finally by requesting them to use some criteria in a harmonized manner.

(2) With reference to Article 35 (4) and (6) GDPR, the competent supervisory authorities shall establish lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment (hereinafter "DPIA"). They shall, however, apply the consistency mechanism where such lists involve processing operations, which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

(3) While the draft lists of the competent supervisory authorities are subject to the consistency mechanism, this does not mean that the lists should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB assessment/opinion is not to reach a single EU list but rather to avoid significant inconsistencies that may affect the equivalent protection of the data subjects.

(4) The carrying out of a DPIA is only mandatory for the controller pursuant to Article 35 (1) GDPR where processing is "likely to result in a high risk to the rights and freedoms of natural

persons". Article 35 (3) GDPR illustrates what is likely to result in a high risk. This is a non-exhaustive list. The Working Party 29 in the Guidelines on data protection impact assessment¹, as endorsed by the EDPB², has clarified criteria that can help to identify when processing operations are subject to the requirement for a DPIA. The Working Party 29 Guidelines WP248 state that in most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out, however, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

(5) The lists produced by the competent supervisory authorities support the same objective to identify processing operations likely to result in a high risk and processing operations, which therefore require a DPIA. As such, the criteria developed in the Working Party 29 Guidelines should be applied when assessing whether the draft lists of the competent supervisory authorities does not affect the consistent application of the GDPR.

(6) Twenty-two competent supervisory authorities have submitted their draft lists to the EDPB. A global assessment of these draft lists supports the objective of a consistent application of the GDPR even though the complexity of the subject matter increases.

(7) The opinion of the EDPB shall be adopted pursuant to Article 64 (3) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

I. Summary of the Facts

The Commission for Personal Data Protection (hereafter Bulgarian Supervisory Authority) has submitted its draft list to the EDPB. The decision on the completeness of the file was taken on 5th July 2018. This period until which the opinion to be adopted has been extended until the 25th of September taking into account the complexity of the subject matter considering that at the same time twenty-two competent supervisory authorities submitted the draft lists and thus the need for a global assessment arose.

¹ WP29, Guidelines on Data Protection Impact Assessment and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP 248 rev. 01).

² EDPB, Endorsement 1/2018.

2. Assessment

2.1 General reasoning of the EDPB regarding the submitted list

Any list submitted to the EDPB has been interpreted as further specifying Art 35.1, which will prevail in any case. Thus, no list can be exhaustive. As the list provided by Bulgarian Supervisory Authority does not explicitly state this, the Board requests this explanation to be added to the document containing the list.

In compliance with article 35.10 GDPR, the Board is of the opinion that if a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of the legal basis the obligation to carry out a DPIA in accordance with paragraphs 1 to 7 of article 35 GDPR does not apply, unless the Member State deems it necessary.

Further, if the Board requests a DPIA for a certain category of processing and an equivalent measure is already required by national law, the Bulgarian Supervisory Authority shall add a reference to this measure.

This opinion does not reflect upon items submitted by the Bulgarian Supervisory Authority, which were deemed outside the scope of Article 35.6 GDPR. This refers to items that neither relate “to the offering of goods or services to data subjects” in several Member States nor to the monitoring of the behaviour of data subjects in several Member States. Additionally, they are not likely to “substantially affect the free movement of personal data within the Union”. This is especially the case for items relating to national legislation and in particular where the obligation to carry out a DPIA is stipulated in national legislation. Further, any processing operations that relate to law enforcement were deemed out of scope, as they are not in scope of the GDPR.

The Board has noted that several supervisory authorities have included in their lists some types of processing which are necessarily local processing. Given that only cross border processing and processing that may affect the free flow of personal data and data subjects are concerned by Article 35.6, the Board will not comment on those local processing.

The opinion aims at defining a consistent core of processing operations that are recurrent in the lists provided by the SAs.

This means that, for a limited number of types of processing operations, that will be defined in a harmonised way, all the Supervisory Authorities will require a DPIA to be carried out and the Board will recommend the SAs to amend their lists accordingly in order to ensure consistency.

When this opinion remains silent on DPIA list entries submitted, it means that the Board is not asking the Bulgarian Supervisory Authority to take further action.

Finally, the Board recalls that transparency is key for data controllers and data processors. In order to clarify the entries in the list, the Board is of the opinion that making an explicit

reference in the lists, for each type of processing, to the criteria set out in the guidelines could improve this transparency. Therefore, the Board considers that an explanation on which criteria have been taken into account by the Bulgarian Supervisory Authority to create its list could be added.

2.2 Application of the consistency mechanism to the draft list

The submitted draft list by the Bulgarian Supervisory Authority relates to the offering of goods or services to data subjects, relates to the monitoring of their behaviour in several Member States and/or may substantially affect the free movement of personal data within the Union mainly because the processing operations in the submitted draft list are not limited to data subjects in this country.

2.3 Analysis of the draft list

Taking into account that:

- a. Article 35 (1) GDPR requires a DPIA when the processing activity is likely to result in a high risk to the rights and freedoms of natural persons; and
- b. Article 35 (3) GDPR provides a non-exhaustive list of types of processing that require a DPIA,

the Board is of the opinion that:

INDICATIVE NATURE OF THE LIST

As the list provided by Bulgarian Supervisory Authority does not explicitly state that its list is not exhaustive, the Board requests this explanation to be added to the document containing the list.

REFERENCE TO THE GUIDELINES

The board is of the opinion that the analysis done in the Working Party 29 Guidelines WP248 are a core element for ensuring consistency across the Union. Thus, it requests the different Supervisor Authorities to add a statement to the document containing their list that clarifies that their list is based on these guidelines and that it complements and further specifies the guidelines.

As the document of the Bulgarian Supervisory Authority does not contain such a statement, the Board recommends the Bulgarian Supervisory Authority to amend its document accordingly.

BIOMETRIC DATA

The list submitted by the Bulgarian Supervisory Authority for an opinion of the Board envisages that the processing of biometric data for the purpose of uniquely identifying a natural person, in conjunction with at least one other criterion, requires a DPIA. On this point, the Board acknowledges that the list aligns with the aim of consistency.

GENETIC DATA

The list submitted by the Bulgarian Supervisory Authority for an opinion of the Board envisages that the processing of genetic data, in conjunction with at least one other criterion, requires a DPIA. The Board is of the opinion that the processing of genetic data on its own is not necessarily likely to represent a high risk. However, the processing of genetic data in conjunction with at least one other criterion requires a DPIA to be carried out. The Board takes note of the inclusion of this criterion in the list of Bulgarian Supervisory Authority.

BIOMETRIC 'AND' GENETIC DATA

The list submitted by the Bulgarian Supervisory Authority for an opinion includes a reference to biometric and genetic data (cumulatively) as a separate entry. The Board has been informed by the Bulgarian Supervisory Authority that in the original language version biometric and genetic data are in fact considered separately. Therefore, the Board refers to the sections in the opinion on biometric data and genetic data respectively.

LOCATION DATA

The Board is of the opinion that consistency is one of the basic principle of the GDPR. The Board notes that a majority of the lists submitted explicitly contain a reference to the processing of location data. As the list submitted by the Bulgarian Supervisory Authority for an opinion do not contain such a reference, the Board encourages the Bulgarian Supervisory Authority to include the processing of location data in its list, together with another criterion.

EXCEPTIONS TO INFORMATION TO BE PROVIDED TO THE DATA SUBJECT ACCORDING TO ARTICLE 14.5 GDPR

The Board is of the opinion that types of processing activities that could deprive the data subjects from their rights do not represent a high risk on their own. Therefore, a processing activity conducted by the controller under article 14 GDPR and where the information to be given to the data subjects is subject to an exemption under article 14.5 (b)-(d) could require a DPIA to be carried out only in conjunction with at least one other criterion. The list submitted by the Bulgarian Supervisory Authority for an opinion of the Board does currently require a DPIA to be done for the processing of data where article 14(5), para (b), (c) and (d) applies on its own. The Board requests the Bulgarian Supervisory Authority to amend its list accordingly, by adapting the list entry by adding that it requires a DPIA only in conjunction with at least one other criterion.

REFERENCING A SPECIFIC LEGAL BASIS

The Board is of the opinion that the use of a specific legal basis should not be a criterion leading to an obligation to do a DPIA, alone or with another criterion. Given that the list submitted by the Bulgarian Supervisory Authority for an opinion of the Board envisages this type of processing as requiring a data protection impact assessment, the Board requests the Bulgarian Supervisory Authority to amend its list accordingly, by removing the reference to any specific legal basis from its list.

JOINT CONTROLLERSHIP

The Board is of the opinion that joint controllership should not be a criterion leading to an obligation to do a DPIA, alone or with another criterion. Thus, the processing of personal data under a joint controllership should not per se require a DPIA to be carried out. The list submitted by the Bulgarian Supervisory Authority for an opinion of the Board does currently require a DPIA to be carried out when there is a processing under a joint controllership. The Board requests the Bulgarian Supervisory Authority to amend its list accordingly, by removing the item of processing under a joint controllership from its list.

TERRITORIALLY-DISTRIBUTED OR CROSS-BORDER INFORMATION SYSTEMS

The Board is of the opinion that processing operations, which are conducted through territorially distributed or cross-border information systems, should not be a criterion leading to an obligation to do a DPIA, alone or with another criterion. Given that the list submitted by the Bulgarian Supervisory Authority for an opinion of the Board envisages this type of processing as requiring a data protection impact assessment, the Board requests the Bulgarian Supervisory Authority to amend its list accordingly, by removing the reference to processing operations which are conducted through territorially-distributed or cross-border information systems from its list.

MIGRATION FROM ONE SYSTEM TO AT LEAST ONE OTHER

The Board is of the opinion that the migration from one system to another on its own is not necessarily likely to represent a high risk. However, the migration from one system to another in conjunction with at least one other criterion does require a DPIA to be carried out. The list submitted by the Bulgarian Supervisory Authority for an opinion of the Board does currently require a DPIA to be carried out when there is a migration from one system to another on its own. The Board requests the Bulgarian Supervisory Authority to amend its list accordingly, by adding that the item referencing the migration from one system to another requires a DPIA to be carried out only when in conjunction with at least one other criterion.

PROCESSING USING NEW/INNOVATIVE TECHNOLOGY

The list submitted by the Bulgarian Supervisory Authority for an opinion of the Board envisages that the processing of personal data using innovative technology in conjunction with at least one other criterion, requires a DPIA. The Board takes note of the inclusion of this criterion in the list.

3. Conclusions / Recommendations

The draft list of the Bulgarian Supervisory Authority may lead to an inconsistent application of the requirement for a DPIA and the following changes need to be made:

- Regarding the indicative nature of the list: the Board requests an explanation to be added to the document containing the list, stating its non-exhaustive nature.
- Regarding the reference to the guidelines: the Board requests the Bulgarian Supervisory Authority to amend its document accordingly.

- Regarding location data: the Board encourages the Bulgarian Supervisory Authority to include the processing of location data in its list, together with another criterion.
- Regarding the exceptions to the information to be given to the data subjects according to article 14.5 GDPR: the Board requests the Bulgarian Supervisory Authority to amend its list by adding that it requires a DPIA only in conjunction with at least one other criterion.
- Regarding the link of a legal basis to high risk: the Board requests the Bulgarian Supervisory Authority to amend its list by removing the reference to any legal basis in its list.
- Regarding joint controllers: the Board requests the Bulgarian Supervisory Authority to amend its list by removing the reference to joint controllership from its list.
- Regarding processing operations which are conducted through territorially-distributed or cross-border information systems: the Board requests the Bulgarian Supervisory Authority to amend its list by removing the reference to processing operations which are conducted through territorially-distributed or cross-border information systems from its list.
- Regarding migration from one system to at least one other: the Board requests the Bulgarian Supervisory Authority to amend its list by adding that the item referencing the migration from one system to another requires a DPIA to be carried out only when in conjunction with at least one other criterion.

4. Final Remarks

This opinion is addressed to the Commission for Personal Data Protection (Bulgarian Supervisory Authority) and will be made public pursuant to Article 64 (5b) GDPR.

According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 4/2018

on the draft list of the competent supervisory authority of Czech Republic

regarding

**the processing operations subject to the requirement of a data protection
impact assessment (Article 35.4 GDPR)**

Adopted on 25th September 2018

Contents

1.	Summary of the Facts	4
2.	Assessment	5
2.1	General reasoning of the EDPB regarding the submitted list	5
2.2	Application of the consistency mechanism to the draft list	6
2.3	Analysis of the draft list.....	6
	Indicative nature of the list.....	6
	Reference to the Guidelines	6
	Biometric data.....	6
	Genetic data.....	7
	Large scale.....	7
	Employee Monitoring	7
	International transfers	7
	First use of solutions applied on the Czech Republic's territory	7
3.	Conclusions / Recommendations	8
4.	Final Remarks	8

The European Data Protection Board

Having regard to Article 63, Article 64 (1a), (3) - (8) and Article 35 (1), (3), (4), (6) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (here after GDPR) throughout the European Economic Area. In compliance with article 64.1 GDPR, the Board has to issue an opinion where a supervisory authority intends to adopt a list of processing operations subject to the requirement for a data protection impact assessment pursuant to article 35.4 GDPR. The aim of this opinion is therefore to create a harmonized approach with regard to processing that is cross border or that can affect the free flow of personal data or natural person across the European Union. Even though the GDPR doesn't impose a single list, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by requesting SAs to include some types of processing in their lists, secondly by requesting them to remove some criteria which the Board doesn't consider as necessarily creating high risks for data subjects, and finally by requesting them to use some criteria in a harmonized manner.

(2) With reference to Article 35 (4) and (6) GDPR, the competent supervisory authorities shall establish lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment (hereinafter "DPIA"). They shall, however, apply the consistency mechanism where such lists involve processing operations, which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

(3) While the draft lists of the competent supervisory authorities are subject to the consistency mechanism, this does not mean that the lists should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB assessment/opinion is not to reach a single EU list but rather to avoid significant inconsistencies that may affect the equivalent protection of the data subjects.

(4) The carrying out of a DPIA is only mandatory for the controller pursuant to Article 35 (1) GDPR where processing is "likely to result in a high risk to the rights and freedoms of natural

persons". Article 35 (3) GDPR illustrates what is likely to result in a high risk. This is a non-exhaustive list. The Working Party 29 in the Guidelines on data protection impact assessment¹, as endorsed by the EDPB², has clarified criteria that can help to identify when processing operations are subject to the requirement for a DPIA. The Working Party 29 Guidelines WP248 state that in most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out, however, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

(5) The lists produced by the competent supervisory authorities support the same objective to identify processing operations likely to result in a high risk and processing operations, which therefore require a DPIA. As such, the criteria developed in the Working Party 29 Guidelines should be applied when assessing whether the draft lists of the competent supervisory authorities does not affect the consistent application of the GDPR.

(6) Twenty-two competent supervisory authorities have submitted their draft lists to the EDPB. A global assessment of these draft lists supports the objective of a consistent application of the GDPR even though the complexity of the subject matter increases.

(7) The opinion of the EDPB shall be adopted pursuant to Article 64 (3) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

I. Summary of the Facts

The Úřad pro ochranu osobních údajů (hereafter Supervisory Authority of the Czech Republic) has submitted its draft list to the EDPB. The decision on the completeness of the file was taken on 25th of June 2018. This period until which the opinion to be adopted has been extended until the 25th of September taking into account the complexity of the subject matter considering that at the same time twenty-two competent supervisory authorities submitted the draft lists and thus the need for a global assessment arose.

¹ WP29, Guidelines on Data Protection Impact Assessment and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP 248 rev. 01).

² EDPB, Endorsement 1/2018.

2. Assessment

2.1 General reasoning of the EDPB regarding the submitted list

Any list submitted to the EDPB has been interpreted as further specifying Art 35.1, which will prevail in any case. Thus, no list can be exhaustive. As the list provided by Supervisory Authority of the Czech Republic does not explicitly state this, the Board requests this explanation to be added to the document containing the list.

In compliance with article 35.10 GDPR, the Board is of the opinion that if a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of the legal basis the obligation to carry out a DPIA in accordance with paragraphs 1 to 7 of article 35 GDPR does not apply, unless the Member State deems it necessary.

Further, if the Board requests a DPIA for a certain category of processing and an equivalent measure is already required by national law, the Supervisory Authority of the Czech Republic shall add a reference to this measure.

This opinion does not reflect upon items submitted by the Supervisory Authority of the Czech Republic, which were deemed outside the scope of Article 35.6 GDPR. This refers to items that neither relate “to the offering of goods or services to data subjects” in several Member States nor to the monitoring of the behaviour of data subjects in several Member States. Additionally, they are not likely to “substantially affect the free movement of personal data within the Union”. This is especially the case for items relating to national legislation and in particular where the obligation to carry out a DPIA is stipulated in national legislation. Further, any processing operations that relate to law enforcement were deemed out of scope, as they are not in scope of the GDPR.

The Board has noted that several supervisory authorities have included in their lists some types of processing which are necessarily local processing. Given that only cross border processing and processing that may affect the free flow of personal data and data subjects are concerned by Article 35.6, the Board will not comment on those local processing.

The opinion aims at defining a consistent core of processing operations that are recurrent in the lists provided by the SAs.

This means that, for a limited number of types of processing operations, that will be defined in a harmonised way, all the Supervisory Authorities will require a DPIA to be carried out and the Board will recommend the SAs to amend their lists accordingly in order to ensure consistency.

When this opinion remains silent on DPIA list entries submitted, it means that the Board is not asking the Supervisory Authority of the Czech Republic to take further action.

Finally, the Board recalls that transparency is key for data controllers and data processors. In order to clarify the entries in the list, the Board is of the opinion that making an explicit

reference in the lists, for each type of processing, to the criteria set out in the guidelines could improve this transparency. Therefore, the Board considers that an explanation on which criteria have been taken into account by the Supervisory Authority of the Czech Republic to create its list could be added.

2.2 Application of the consistency mechanism to the draft list

The submitted draft list by the Supervisory Authority of the Czech Republic relates to the offering of goods or services to data subjects, relates to the monitoring of their behaviour in several Member States and/or may substantially affect the free movement of personal data within the Union mainly because the processing operations in the submitted draft list are not limited to data subjects in this country.

2.3 Analysis of the draft list

Taking into account that:

- a. Article 35 (1) GDPR requires a DPIA when the processing activity is likely to result in a high risk to the rights and freedoms of natural persons; and
- b. Article 35 (3) GDPR provides a non-exhaustive list of types of processing that require a DPIA,

the Board is of the opinion that:

INDICATIVE NATURE OF THE LIST

As the list provided by Supervisory Authority of the Czech Republic does not explicitly state that its list is not exhaustive, the Board requests this explanation to be added to the document containing the list.

REFERENCE TO THE GUIDELINES

The board is of the opinion that the analysis done in the Working Party 29 Guidelines WP248 are a core element for ensuring consistency across the Union. Thus, it requests the different Supervisor Authorities to add a statement to the document containing their list that clarifies that their list is based on these guidelines and that it complements and further specifies the guidelines.

Although the document of the Supervisory Authority of the Czech Republic does include a reference to the Guidelines, the Board recommends the Supervisory Authority of the Czech Republic to further clarify the link between its document and the WP 29 guidelines.

BIOMETRIC DATA

The list submitted by the Supervisory Authority of the Czech Republic for an opinion of the Board envisages that the processing of biometric data for the purpose of uniquely identifying a natural person, in conjunction with at least one other criterion, requires a DPIA. On this point, the Board acknowledges that the list aligns with the aim of consistency.

GENETIC DATA

The list submitted by the Supervisory Authority of the Czech Republic for an opinion of the Board envisages that the processing of genetic data, in conjunction with at least one other criterion, requires a DPIA. The Board is of the opinion that the processing of genetic data on its own is not necessarily likely to represent a high risk. However, the processing of genetic data in conjunction with at least one other criterion requires a DPIA to be carried out. The Board takes note of the inclusion of this criterion in the list of Supervisory Authority of the Czech Republic.

LARGE SCALE

The GDPR does not precisely define what constitutes large-scale. In the WP29 guidelines on Data Protection Officer (WP243) and on DPIA (WP248), both endorsed by Board, it has recommended to take in account several specific factors when determining whether a processing is carried out on a large scale.

The Board is of the opinion that those factors are sufficient to assess whether the processing of personal data is undertaken on a large scale. Therefore, the Board requests the Supervisory Authority of the Czech Republic to amend its list accordingly, by deleting the explicit figures in its list, and making reference to the previously mentioned definitions of large scale.

EMPLOYEE MONITORING

The Board is of the opinion that, due to its specific nature, the employee monitoring processing, meeting the criterion of vulnerable data subjects and of systematic monitoring in the guidelines, – could require a DPIA. Given that the list submitted by the Supervisory Authority of the Czech Republic for an opinion of the Board already envisages this type of processing as requiring a data protection impact assessment, the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248. In addition, the Board is of the opinion that the WP249 of the Article 29 working party remains valid when defining the concept of the systematic processing of employee data.

INTERNATIONAL TRANSFERS

The Board is of the opinion that the processing made in the context of international transfers should not be a criterion leading to an obligation to do a DPIA, alone or with another criterion. Given that the list submitted by the Supervisory Authority of the Czech Republic for an opinion of the Board envisages this type of processing as requiring a data protection impact assessment, the Board requests the Supervisory Authority of the Czech Republic to amend its list accordingly, by removing the reference to international transfers from its list.

FIRST USE OF SOLUTIONS APPLIED ON THE CZECH REPUBLIC'S TERRITORY

The Board is of the opinion that the definition of innovative technology in its item 11, in particular the first application of solutions applied on the Czech Republic's territory, is problematic as high risk is not correlated necessarily with first application. Given that the list submitted by the Supervisory Authority of the Czech Republic for an opinion of the Board envisages this type of processing as requiring, on its own, a data protection impact

assessment, the Board requests the Supervisory Authority of the Czech Republic to amend its list accordingly, by aligning the definition of innovative technology in its item 11 to the WP29 248 guidelines, in particular by removing the qualifier of ‘first application’.

3. Conclusions / Recommendations

The draft list of the Supervisory Authority of the Czech Republic may lead to an inconsistent application of the requirement for a DPIA and the following changes need to made:

- Regarding the indicative nature of the list: the Board requests an explanation to be added to the document containing the list, stating its non-exhaustive nature.
- Regarding the reference to the guidelines: the Board requests the Supervisory Authority of the Czech Republic to amend its document accordingly.
- Regarding the notion of large scale: the Board requests the Supervisory Authority of the Czech Republic to amend its list by deleting the explicit figures in its list, and making reference to the definitions of large scale mentioned in the WP29 guidelines on Data Protection Officer (WP243) and on DPIA (WP248).
- Regarding employment monitoring: the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248.
- Regarding international transfers: Board requests the Supervisory Authority of the Czech Republic to amend its list by removing the reference to international transfers from its list.
- Regarding the first use of solutions applied on the Czech Republic’s territory: the Board requests the Supervisory Authority of the Czech Republic to amend its list by aligning the definition of innovative technology in its item 11 to the WP29 248 guidelines, in particular by removing the qualifier of ‘first application’.

4. Final Remarks

This opinion is addressed to the Úřad pro ochranu osobních údajů (Supervisory Authority of the Czech Republic) and will be made public pursuant to Article 64 (5b) GDPR.

According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 5/2018

on the draft list of the competent supervisory authorities of Germany

regarding

**the processing operations subject to the requirement of a data protection
impact assessment (Article 35.4 GDPR)**

Adopted on 25th September 2018

Contents

1.	Summary of the Facts	4
2.	Assessment	5
2.1	General reasoning of the EDPB regarding the submitted list	5
2.2	Application of the consistency mechanism to the draft list	6
2.3	Analysis of the draft list.....	6
	Indicative nature of the list.....	6
	Reference to the Guidelines	6
	Biometric data.....	6
	Genetic data.....	7
	Location data	7
	Data collected via third parties (article 19 GDPR)	7
	Further processing	7
	Employee Monitoring	8
	Interfaces of personal electronic Device unprotected against unauthorized readout	8
3.	Conclusions / Recommendations	8
4.	Final Remarks.....	9

The European Data Protection Board

Having regard to Article 63, Article 64 (1a), (3) - (8) and Article 35 (1), (3), (4), (6) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (here after GDPR) throughout the European Economic Area. In compliance with article 64.1 GDPR, the Board has to issue an opinion where a supervisory authority intends to adopt a list of processing operations subject to the requirement for a data protection impact assessment pursuant to article 35.4 GDPR. The aim of this opinion is therefore to create a harmonized approach with regard to processing that is cross border or that can affect the free flow of personal data or natural person across the European Union. Even though the GDPR doesn't impose a single list, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by requesting SAs to include some types of processing in their lists, secondly by requesting them to remove some criteria which the Board doesn't consider as necessarily creating high risks for data subjects, and finally by requesting them to use some criteria in a harmonized manner.

(2) With reference to Article 35 (4) and (6) GDPR, the competent supervisory authorities shall establish lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment (hereinafter "DPIA"). They shall, however, apply the consistency mechanism where such lists involve processing operations, which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

(3) While the draft lists of the competent supervisory authorities are subject to the consistency mechanism, this does not mean that the lists should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB assessment/opinion is not to reach a single EU list but rather to avoid significant inconsistencies that may affect the equivalent protection of the data subjects.

(4) The carrying out of a DPIA is only mandatory for the controller pursuant to Article 35 (1) GDPR where processing is "likely to result in a high risk to the rights and freedoms of natural

persons". Article 35 (3) GDPR illustrates what is likely to result in a high risk. This is a non-exhaustive list. The Working Party 29 in the Guidelines on data protection impact assessment¹, as endorsed by the EDPB², has clarified criteria that can help to identify when processing operations are subject to the requirement for a DPIA. The Working Party 29 Guidelines

WP248 state that in most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out, however, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

(5) The lists produced by the competent supervisory authorities support the same objective to identify processing operations likely to result in a high risk and processing operations, which therefore require a DPIA. As such, the criteria developed in the Working Party 29 Guidelines should be applied when assessing whether the draft lists of the competent supervisory authorities does not affect the consistent application of the GDPR.

(6) Twenty-two competent supervisory authorities have submitted their draft lists to the EDPB. A global assessment of these draft lists supports the objective of a consistent application of the GDPR even though the complexity of the subject matter increases.

(7) The opinion of the EDPB shall be adopted pursuant to Article 64 (3) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

I. Summary of the Facts

The Bundesbeauftragte und die Aufsichtsbehörden der Länder (hereafter Supervisory Authorities of the Federation and the Länder) have submitted its draft list to the EDPB. The decision on the completeness of the file was taken on 11th July 2018. This period until which the opinion to be adopted has been extended until the 25th of September taking into account the complexity of the subject matter considering that at the same time twenty-two competent supervisory authorities submitted the draft lists and thus the need for a global assessment arose.

¹ WP29, Guidelines on Data Protection Impact Assessment and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP 248 rev. 01).

² EDPB, Endorsement 1/2018.

2. Assessment

2.1 General reasoning of the EDPB regarding the submitted list

Any list submitted to the EDPB has been interpreted as further specifying Art 35.1, which will prevail in any case. Thus, no list can be exhaustive. As the list provided by Supervisory Authorities of the Federation and the Länder does not explicitly state this, the Board requests this explanation to be added to the document containing the list.

In compliance with article 35.10 GDPR, the Board is of the opinion that if a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of the legal basis the obligation to carry out a DPIA in accordance with paragraphs 1 to 7 of article 35 GDPR does not apply, unless the Member State deems it necessary.

Further, if the Board requests a DPIA for a certain category of processing and an equivalent measure is already required by national law, the Supervisory Authorities of the Federation and the Länder shall add a reference to this measure.

This opinion does not reflect upon items submitted by the Supervisory Authorities of the Federation and the Länder, which were deemed outside the scope of Article 35.6 GDPR. This refers to items that neither relate “to the offering of goods or services to data subjects” in several Member States nor to the monitoring of the behaviour of data subjects in several Member States. Additionally, they are not likely to “substantially affect the free movement of personal data within the Union”. This is especially the case for items relating to national legislation and in particular where the obligation to carry out a DPIA is stipulated in national legislation. Further, any processing operations that relate to law enforcement were deemed out of scope, as they are not in scope of the GDPR.

The Board has noted that several supervisory authorities have included in their lists some types of processing which are necessarily local processing. Given that only cross border processing and processing that may affect the free flow of personal data and data subjects are concerned by Article 35.6, the Board will not comment on those local processing.

The opinion aims at defining a consistent core of processing operations that are recurrent in the lists provided by the SAs.

This means that, for a limited number of types of processing operations, that will be defined in a harmonised way, all the Supervisory Authorities will require a DPIA to be carried out and the Board will recommend the SAs to amend their lists accordingly in order to ensure consistency.

When this opinion remains silent on DPIA list entries submitted, it means that the Board is not asking the Supervisory Authorities of the Federation and the Länder to take further action.

Finally, the Board recalls that transparency is key for data controllers and data processors. In order to clarify the entries in the list, the Board is of the opinion that making an explicit

reference in the lists, for each type of processing, to the criteria set out in the guidelines could improve this transparency. Therefore, the Board considers that an explanation on which criteria have been taken into account by the Supervisory Authorities of the Federation and the Länder to create its list could be added.

2.2 Application of the consistency mechanism to the draft list

The submitted draft list by the Supervisory Authorities of the Federation and the Länder relates to the offering of goods or services to data subjects, relates to the monitoring of their behaviour in several Member States and/or may substantially affect the free movement of personal data within the Union mainly because the processing operations in the submitted draft list are not limited to data subjects in this country.

2.3 Analysis of the draft list

Taking into account that:

- a. Article 35 (1) GDPR requires a DPIA when the processing activity is likely to result in a high risk to the rights and freedoms of natural persons; and
- b. Article 35 (3) GDPR provides a non-exhaustive list of types of processing that require a DPIA,

the Board is of the opinion that:

INDICATIVE NATURE OF THE LIST

As the list provided by Supervisory Authorities of the Federation and the Länder does not explicitly state that its list is not exhaustive, the Board requests this explanation to be added to the document containing the list.

REFERENCE TO THE GUIDELINES

The board is of the opinion that the analysis done in the Working Party 29 Guidelines WP248 are a core element for ensuring consistency across the Union. Thus, it requests the different Supervisor Authorities to add a statement to the document containing their list that clarifies that their list is based on these guidelines and that it complements and further specifies the guidelines.

As the document of the Supervisory Authorities of the Federation and the Länder does not contain such a statement, the Board recommends the Supervisory Authorities of the Federation and the Länder to amend their document accordingly.

BIOMETRIC DATA

The list submitted by the Supervisory Authorities of the Federation and the Länder for an opinion of the Board does not currently require a DPIA to be done for the processing of biometric data for the purpose of uniquely identifying a natural person. As such, the Board requests the Supervisory Authorities of the Federation and the Länder to amend its list accordingly, by adding explicitly the processing of biometric data for the purpose of uniquely identifying a natural person in conjunction with at least one other criterion to its list, to be applied without prejudice to article 35(3) GDPR.

GENETIC DATA

The list submitted by the Supervisory Authorities of the Federation and the Länder for an opinion of the Board does not currently require a DPIA to be done for the processing of genetic data. . The Board is of the opinion that the processing of genetic data on its own is not necessarily likely to represent a high risk. However, the processing of genetic data in conjunction with at least one other criterion requires a DPIA to be carried out. As such, the Board requests the Supervisory Authorities of the Federation and the Länder to amend its list accordingly, by adding explicitly the processing of genetic data in conjunction with at least one other criterion to its list, to be applied without prejudice to article 35(3) GDPR.

LOCATION DATA

The Board is of the opinion that the processing of location data on its own is not necessarily likely to represent a high risk. However, the processing of location data in conjunction with at least one other criterion requires a DPIA to be carried out. The list submitted by the Supervisory Authorities of the Federation and the Länder for an opinion of the Board does currently require a DPIA to be carried out when there is a processing of location data on its own. The Board requests the Supervisory Authorities of the Federation and the Länder to amend its list accordingly, by adding that the item referencing the processing of location data requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.

DATA COLLECTED VIA THIRD PARTIES (ARTICLE 19 GDPR)

The Board is of the opinion that types of processing activities that could deprive the data subjects from their rights on their own do not represent a high risk. Further, the Board is of the opinion that a processing activity conducted by the controller under article 19 GDPR and where the information of recipients would prove impossible or require a disproportionate effort only requires a DPIA to be carried out when this processing involves at least one other criterion. The list submitted by the Supervisory Authorities of the Federation and the Länder for an opinion of the Board states that this type of processing on its own falls under the obligation to perform a DPIA. The Board requests the Supervisory Authorities of the Federation and the Länder to amend its list accordingly, by adding that the item referencing the processing of personal data collected via third parties requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.

FURTHER PROCESSING

The Board is of the opinion that further processing of personal data should not be a criterion leading to an obligation to do a DPIA, alone or with another criterion. The list submitted by the Supervisory Authorities of the Federation and the Länder for an opinion of the Board does currently require a DPIA to be carried out for the further processing of personal data. The Board requests the Supervisory Authorities of the Federation and the Länder to amend its list accordingly, by removing this criterion.

EMPLOYEE MONITORING

The Board is of the opinion that, due to its specific nature, the employee monitoring processing, meeting the criterion of vulnerable data subjects and of systematic monitoring in the guidelines, – could require a DPIA. Given that the list submitted by the Supervisory Authorities of the Federation and the Länder for an opinion of the Board already envisages this type of processing as requiring a data protection impact assessment, the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248. In addition, the Board is of the opinion that the WP249 of the Article 29 working party remains valid when defining the concept of the systematic processing of employee data.

INTERFACES OF PERSONAL ELECTRONIC DEVICE UNPROTECTED AGAINST UNAUTHORIZED READOUT

The Board is of the opinion that the processing made in the context of the collection of personal data via interfaces of personal electronic devices, which are not protected against unauthorized readout, should not be a criterion leading to an obligation to do a DPIA, alone or with another criterion. Given that the list submitted by the Supervisory Authorities of the Federation and the Länder for an opinion of the Board envisages this type of processing as requiring a data protection impact assessment, the Board requests the Supervisory Authorities of the Federation and the Länder to amend its list accordingly, by removing the reference to the collection of personal data via interfaces of personal electronic devices which are not protected against unauthorized readout from its list.

3. Conclusions / Recommendations

The draft list of the Supervisory Authorities of the Federation and the Länder may lead to an inconsistent application of the requirement for a DPIA and the following changes need to be made:

- Regarding the indicative nature of the list: the Board requests an explanation to be added to the document containing the list, stating its non-exhaustive nature.
- Regarding the reference to the guidelines: the Board requests the Supervisory Authorities of the Federation and the Länder to amend their document accordingly.
- Regarding biometric data: the Board requests the Supervisory Authorities of the Federation and the Länder to amend its list by adding explicitly the processing of biometric data for the purpose of uniquely identifying a natural person in conjunction with at least one other criterion to its list.
- Regarding genetic data: the Board requests the Supervisory Authorities of the Federation and the Länder to amend its list by adding explicitly the processing of genetic data in conjunction with at least one other criterion to its list.
- Regarding location data: the Board requests the Supervisory Authorities of the Federation and the Länder to amend its list by adding that the item referencing the processing of location data requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.

- Regarding the data collected via third parties (article 19 GDPR): the Board requests the Supervisory Authorities of the Federation and the Länder to amend its list by adding that the item referencing the processing of personal data collected via third parties requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.
- Regarding further processing: the Board requests the Supervisory Authorities of the Federation and the Länder to amend its list accordingly, by removing this criterion.
- Regarding employment monitoring: the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248.
- Regarding the processing made in the context of the collection of personal data via interfaces of personal electronic devices which are not protected against unauthorized readout: the Board requests the Supervisory Authorities of the Federation and the Länder to amend its list by removing the reference to the collection of personal data via interfaces of personal electronic devices which are not protected against unauthorized readout from its list

4. Final Remarks

This opinion is addressed to the Bundesbeauftragte und die Aufsichtsbehörden der Länder (supervisory authorities of the Federation and the Länder) and will be made public pursuant to Article 64 (5b) GDPR.

According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 6/2018

on the draft list of the competent supervisory authority of Estonia

regarding

**the processing operations subject to the requirement of a data protection
impact assessment (Article 35.4 GDPR)**

Adopted on 25th September 2018

Contents

1.	Summary of the Facts	4
2.	Assessment	5
2.1	General reasoning of the EDPB regarding the submitted list	5
2.2	Application of the consistency mechanism to the draft list	6
2.3	Analysis of the draft list.....	6
	Indicative nature of the list.....	6
	Reference to the Guidelines	6
	Biometric data.....	6
	Genetic data.....	7
	Large scale.....	7
	Employee Monitoring	7
3.	Conclusions / Recommendations	7
4.	Final Remarks.....	8

The European Data Protection Board

Having regard to Article 63, Article 64 (1a), (3) - (8) and Article 35 (1), (3), (4), (6) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (here after GDPR) throughout the European Economic Area. In compliance with article 64.1 GDPR, the Board has to issue an opinion where a supervisory authority intends to adopt a list of processing operations subject to the requirement for a data protection impact assessment pursuant to article 35.4 GDPR. The aim of this opinion is therefore to create a harmonized approach with regard to processing that is cross border or that can affect the free flow of personal data or natural person across the European Union. Even though the GDPR doesn't impose a single list, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by requesting SAs to include some types of processing in their lists, secondly by requesting them to remove some criteria which the Board doesn't consider as necessarily creating high risks for data subjects, and finally by requesting them to use some criteria in a harmonized manner..

(2) With reference to Article 35 (4) and (6) GDPR, the competent supervisory authorities shall establish lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment (hereinafter "DPIA"). They shall, however, apply the consistency mechanism where such lists involve processing operations, which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

(3) While the draft lists of the competent supervisory authorities are subject to the consistency mechanism, this does not mean that the lists should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB assessment/opinion is not to reach a single EU list but rather to avoid significant inconsistencies that may affect the equivalent protection of the data subjects.

(4) The carrying out of a DPIA is only mandatory for the controller pursuant to Article 35 (1) GDPR where processing is "likely to result in a high risk to the rights and freedoms of natural

persons". Article 35 (3) GDPR illustrates what is likely to result in a high risk. This is a non-exhaustive list. The Working Party 29 in the Guidelines on data protection impact assessment¹, as endorsed by the EDPB², has clarified criteria that can help to identify when processing operations are subject to the requirement for a DPIA. The Working Party 29 Guidelines WP248 state that in most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out, however, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

(5) The lists produced by the competent supervisory authorities support the same objective to identify processing operations likely to result in a high risk and processing operations, which therefore require a DPIA. As such, the criteria developed in the Working Party 29 Guidelines should be applied when assessing whether the draft lists of the competent supervisory authorities does not affect the consistent application of the GDPR.

(6) Twenty-two competent supervisory authorities have submitted their draft lists to the EDPB. A global assessment of these draft lists supports the objective of a consistent application of the GDPR even though the complexity of the subject matter increases.

(7) The opinion of the EDPB shall be adopted pursuant to Article 64 (3) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

I. Summary of the Facts

The Andmekaitse Inspeksiõon (hereafter Estonian Supervisory Authority) has submitted its draft list to the EDPB. The decision on the completeness of the file was taken on 20th of June 2018. This period until which the opinion to be adopted has been extended until the 25th of September taking into account the complexity of the subject matter considering that at the same time twenty-two competent supervisory authorities submitted the draft lists and thus the need for a global assessment arose.

¹ WP29, Guidelines on Data Protection Impact Assessment and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP 248 rev. 01).

² EDPB, Endorsement 1/2018.

2. Assessment

2.1 General reasoning of the EDPB regarding the submitted list

Any list submitted to the EDPB has been interpreted as further specifying Art 35.1, which will prevail in any case. Thus, no list can be exhaustive. As the list provided by Estonian Supervisory Authority does not explicitly state this, the Board requests this explanation to be added to the document containing the list.

In compliance with article 35.10 GDPR, the Board is of the opinion that if a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of the legal basis the obligation to carry out a DPIA in accordance with paragraphs 1 to 7 of article 35 GDPR does not apply, unless the Member State deems it necessary.

Further, if the Board requests a DPIA for a certain category of processing and an equivalent measure is already required by national law, the Estonian Supervisory Authority shall add a reference to this measure.

This opinion does not reflect upon items submitted by the Estonian Supervisory Authority, which were deemed outside the scope of Article 35.6 GDPR. This refers to items that neither relate “to the offering of goods or services to data subjects” in several Member States nor to the monitoring of the behaviour of data subjects in several Member States. Additionally, they are not likely to “substantially affect the free movement of personal data within the Union”. This is especially the case for items relating to national legislation and in particular where the obligation to carry out a DPIA is stipulated in national legislation. Further, any processing operations that relate to law enforcement were deemed out of scope, as they are not in scope of the GDPR.

The Board has noted that several supervisory authorities have included in their lists some types of processing which are necessarily local processing. Given that only cross border processing and processing that may affect the free flow of personal data and data subjects are concerned by Article 35.6, the Board will not comment on those local processing.

The opinion aims at defining a consistent core of processing operations that are recurrent in the lists provided by the SAs.

This means that, for a limited number of types of processing operations, that will be defined in a harmonised way, all the Supervisory Authorities will require a DPIA to be carried out and the Board will recommend the SAs to amend their lists accordingly in order to ensure consistency.

When this opinion remains silent on DPIA list entries submitted, it means that the Board is not asking the Estonian Supervisory Authority to take further action.

Finally, the Board recalls that transparency is key for data controllers and data processors. In order to clarify the entries in the list, the Board is of the opinion that making an explicit

reference in the lists, for each type of processing, to the criteria set out in the guidelines could improve this transparency. Therefore, the Board considers that an explanation on which criteria have been taken into account by the Estonian Supervisory Authority to create its list could be added.

2.2 Application of the consistency mechanism to the draft list

The submitted draft list by the Estonian Supervisory Authority relates to the offering of goods or services to data subjects, relates to the monitoring of their behaviour in several Member States and/or may substantially affect the free movement of personal data within the Union mainly because the processing operations in the submitted draft list are not limited to data subjects in this country.

2.3 Analysis of the draft list

Taking into account that:

- a. Article 35 (1) GDPR requires a DPIA when the processing activity is likely to result in a high risk to the rights and freedoms of natural persons; and
- b. Article 35 (3) GDPR provides a non-exhaustive list of types of processing that require a DPIA,

the Board is of the opinion that:

INDICATIVE NATURE OF THE LIST

As the list provided by Estonian Supervisory Authority does not explicitly state that its list is not exhaustive, the Board requests this explanation to be added to the document containing the list.

REFERENCE TO THE GUIDELINES

The board is of the opinion that the analysis done in the Working Party 29 Guidelines WP248 are a core element for ensuring consistency across the Union. Thus, it requests the different Supervisor Authorities to add a statement to the document containing their list that clarifies that their list is based on these guidelines and that it complements and further specifies the guidelines.

As the document of the Estonian Supervisory Authority does not contain such a statement, the Board recommends the Estonian Supervisory Authority to amend its document accordingly.

BIOMETRIC DATA

The list submitted by the Estonian Supervisory Authority for an opinion of the Board does not currently require a DPIA to be done for the processing of biometric data for the purpose of uniquely identifying a natural person. As such, the Board requests the Estonian Supervisory Authority to amend its list accordingly, by adding explicitly the processing of biometric data for the purpose of uniquely identifying a natural person in conjunction with at least one other criterion to its list, to be applied without prejudice to article 35(3) GDPR.

GENETIC DATA

The list submitted by the Estonian Supervisory Authority for an opinion of the Board does not currently require a DPIA to be done for the processing of genetic data. . The Board is of the opinion that the processing of genetic data on its own is not necessarily likely to represent a high risk. However, the processing of genetic data in conjunction with at least one other criterion requires a DPIA to be carried out. As such, the Board requests the Estonian Supervisory Authority to amend its list accordingly, by adding explicitly the processing of genetic data in conjunction with at least one other criterion to its list, to be applied without prejudice to article 35(3) GDPR.

LARGE SCALE

The GDPR does not precisely define what constitutes large-scale. In the WP29 guidelines on Data Protection Officer and on DPIA, both endorsed by Board, it has recommended to take in account several specific factors when determining whether a processing is carried out on a large scale.

The Board is of the opinion that those factors are sufficient to assess whether the processing of personal data is undertaken on a large scale. Therefore the Board requests the Estonian Supervisory Authority to amend its list accordingly, by deleting the explicit figures in its list, and making reference to the previously mentioned definitions of large scale.

EMPLOYEE MONITORING

The Board is of the opinion that, due to its specific nature, the employee monitoring processing, meeting the criterion of vulnerable data subjects and of systematic monitoring in the guidelines, – could require a DPIA. Given that the list submitted by the Estonian Supervisory Authority for an opinion of the Board already envisages this type of processing as requiring a data protection impact assessment, the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248. In addition, the Board is of the opinion that the WP249 of the Article 29 working party remains valid when defining the concept of the systematic processing of employee data.

3. Conclusions / Recommendations

The draft list of the Estonian Supervisory Authority may lead to an inconsistent application of the requirement for a DPIA and the following changes need to made:

- Regarding the indicative nature of the list: the Board requests an explanation to be added to the document containing the list, stating its non-exhaustive nature.
- Regarding the reference to the guidelines: the Board requests the Estonian Supervisory Authority to amend its document accordingly.
- Regarding biometric data: the Board requests the Estonian Supervisory Authority to amend its list accordingly, by adding explicitly the processing of biometric data for the purpose of uniquely identifying a natural person in conjunction with at least one other criterion to its list.

- Regarding genetic data: the Board requests the Estonian Supervisory Authority to amend its list by adding explicitly the processing of genetic data in conjunction with at least one other criterion to its list.
- Regarding the notion of large scale: the Board requests the Estonian Supervisory Authority to amend its list by deleting the explicit figures in its list, and making reference to the definitions of large scale mentioned in the WP29 guidelines on Data Protection Officer (WP243) and on DPIA (WP248).
- Regarding employment monitoring: the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248.

4. Final Remarks

This opinion is addressed to the Andmekaitse Inspeksioon (Estonian Supervisory Authority) and will be made public pursuant to Article 64 (5b) GDPR.

According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 8/2018

on the draft list of the competent supervisory authority of Finland

regarding

**the processing operations subject to the requirement of a data protection
impact assessment (Article 35.4 GDPR)**

Adopted on 25th September 2018

Contents

1.	Summary of the Facts	4
2.	Assessment	5
2.1	General reasoning of the EDPB regarding the submitted list	5
2.2	Application of the consistency mechanism to the draft list	6
2.3	Analysis of the draft list.....	6
	Indicative nature of the list.....	6
	Reference to the Guidelines	6
	Biometric data.....	6
	Genetic data.....	7
	Location data	7
	Exceptions to information to be provided to the data subject according to article 14.5 GDPR	7
3.	Conclusions / Recommendations	7
4.	Final Remarks.....	8

The European Data Protection Board

Having regard to Article 63, Article 64 (1a), (3) - (8) and Article 35 (1), (3), (4), (6) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (here after GDPR) throughout the European Economic Area. In compliance with article 64.1 GDPR, the Board has to issue an opinion where a supervisory authority intends to adopt a list of processing operations subject to the requirement for a data protection impact assessment pursuant to article 35.4 GDPR. The aim of this opinion is therefore to create a harmonized approach with regard to processing that is cross border or that can affect the free flow of personal data or natural person across the European Union. Even though the GDPR doesn't impose a single list, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by requesting SAs to include some types of processing in their lists, secondly by requesting them to remove some criteria which the Board doesn't consider as necessarily creating high risks for data subjects, and finally by requesting them to use some criteria in a harmonized manner.

(2) With reference to Article 35 (4) and (6) GDPR, the competent supervisory authorities shall establish lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment (hereinafter "DPIA"). They shall, however, apply the consistency mechanism where such lists involve processing operations, which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

(3) While the draft lists of the competent supervisory authorities are subject to the consistency mechanism, this does not mean that the lists should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB assessment/opinion is not to reach a single EU list but rather to avoid significant inconsistencies that may affect the equivalent protection of the data subjects.

(4) The carrying out of a DPIA is only mandatory for the controller pursuant to Article 35 (1) GDPR where processing is "likely to result in a high risk to the rights and freedoms of natural

persons". Article 35 (3) GDPR illustrates what is likely to result in a high risk. This is a non-exhaustive list. The Working Party 29 in the Guidelines on data protection impact assessment¹, as endorsed by the EDPB², has clarified criteria that can help to identify when processing operations are subject to the requirement for a DPIA. The Working Party 29 Guidelines WP248 state that in most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out, however, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

(5) The lists produced by the competent supervisory authorities support the same objective to identify processing operations likely to result in a high risk and processing operations, which therefore require a DPIA. As such, the criteria developed in the Working Party 29 Guidelines should be applied when assessing whether the draft lists of the competent supervisory authorities does not affect the consistent application of the GDPR.

(6) Twenty-two competent supervisory authorities have submitted their draft lists to the EDPB. A global assessment of these draft lists supports the objective of a consistent application of the GDPR even though the complexity of the subject matter increases.

(7) The opinion of the EDPB shall be adopted pursuant to Article 64 (3) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

I. Summary of the Facts

The Tietosuojavaltuutetun toimisto (hereafter Finnish Supervisory Authority) has submitted its draft list to the EDPB. The decision on the completeness of the file was taken on the 27th June 2018. This period until which the opinion to be adopted has been extended until the 25th of September taking into account the complexity of the subject matter considering that at the same time twenty-two competent supervisory authorities submitted the draft lists and thus the need for a global assessment arose.

¹ WP29, Guidelines on Data Protection Impact Assessment and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP 248 rev. 01).

² EDPB, Endorsement 1/2018.

2. Assessment

2.1 General reasoning of the EDPB regarding the submitted list

Any list submitted to the EDPB has been interpreted as further specifying Art 35.1, which will prevail in any case. Thus, no list can be exhaustive. As the list provided by Finnish Supervisory Authority does not explicitly state this, the Board requests this explanation to be added to the document containing the list.

In compliance with article 35.10 GDPR, the Board is of the opinion that if a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of the legal basis the obligation to carry out a DPIA in accordance with paragraphs 1 to 7 of article 35 GDPR does not apply, unless the Member State deems it necessary.

Further, if the Board requests a DPIA for a certain category of processing and an equivalent measure is already required by national law, the Finnish Supervisory Authority shall add a reference to this measure.

This opinion does not reflect upon items submitted by the Finnish Supervisory Authority, which were deemed outside the scope of Article 35.6 GDPR. This refers to items that neither relate “to the offering of goods or services to data subjects” in several Member States nor to the monitoring of the behaviour of data subjects in several Member States. Additionally, they are not likely to “substantially affect the free movement of personal data within the Union”. This is especially the case for items relating to national legislation and in particular where the obligation to carry out a DPIA is stipulated in national legislation. Further, any processing operations that relate to law enforcement were deemed out of scope, as they are not in scope of the GDPR.

The Board has noted that several supervisory authorities have included in their lists some types of processing which are necessarily local processing. Given that only cross border processing and processing that may affect the free flow of personal data and data subjects are concerned by Article 35.6, the Board will not comment on those local processing.

The opinion aims at defining a consistent core of processing operations that are recurrent in the lists provided by the SAs.

This means that, for a limited number of types of processing operations, that will be defined in a harmonised way, all the Supervisory Authorities will require a DPIA to be carried out and the Board will recommend the SAs to amend their lists accordingly in order to ensure consistency.

When this opinion remains silent on DPIA list entries submitted, it means that the Board is not asking the Finnish Supervisory Authority to take further action.

Finally, the Board recalls that transparency is key for data controllers and data processors. In order to clarify the entries in the list, the Board is of the opinion that making an explicit

reference in the lists, for each type of processing, to the criteria set out in the guidelines could improve this transparency. Therefore, the Board considers that an explanation on which criteria have been taken into account by the Finnish Supervisory Authority to create its list could be added.

2.2 Application of the consistency mechanism to the draft list

The submitted draft list by the Finnish Supervisory Authority relates to the offering of goods or services to data subjects, relates to the monitoring of their behaviour in several Member States and/or may substantially affect the free movement of personal data within the Union mainly because the processing operations in the submitted draft list are not limited to data subjects in this country.

2.3 Analysis of the draft list

Taking into account that:

- a. Article 35 (1) GDPR requires a DPIA when the processing activity is likely to result in a high risk to the rights and freedoms of natural persons; and
- b. Article 35 (3) GDPR provides a non-exhaustive list of types of processing that require a DPIA,

the Board is of the opinion that:

INDICATIVE NATURE OF THE LIST

As the list provided by Finnish Supervisory Authority does not explicitly state that its list is not exhaustive, the Board requests this explanation to be added to the document containing the list.

REFERENCE TO THE GUIDELINES

The board is of the opinion that the analysis done in the Working Party 29 Guidelines WP 248 are a core element for ensuring consistency across the Union. Thus, it requests the different Supervisor Authorities to add a statement to the document containing their list that clarifies that their list is based on these guidelines and that it complements and further specifies the guidelines.

As the document of the Finnish Supervisory Authority does not contain such a statement, the Board recommends the Finnish Supervisory Authority to amend its document accordingly.

BIOMETRIC DATA

The list submitted by the Finnish Supervisory Authority for an opinion of the Board does not currently require a DPIA to be done for the processing of biometric data for the purpose of uniquely identifying a natural person. As such, the Board requests the Finnish Supervisory Authority to amend its list accordingly, by adding explicitly the processing of biometric data for the purpose of uniquely identifying a natural person in conjunction with at least one other criterion to its list, to be applied without prejudice to article 35(3) GDPR.

GENETIC DATA

The list submitted by the Finnish Supervisory Authority for an opinion of the Board states, that the processing of genetic data falls under the obligation to perform a DPIA on its own. The Board is of the opinion that the processing of genetic data on its own is not necessarily likely to represent a high risk. However, the processing of genetic data in conjunction with at least one other criterion requires a DPIA to be carried out. As such, the Board requests the Finnish Supervisory Authority to amend its list accordingly, by adding that the item referencing the processing of genetic data requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion, to be applied without prejudice to article 35(3) GDPR.

LOCATION DATA

The Board is of the opinion that consistency is one of the basic principle of the GDPR. The Board notes that a majority of the lists submitted explicitly contain a reference to the processing of location data. As the list submitted by the Finnish Supervisory Authority for an opinion do not contain such a reference, the Board encourages the Finnish Supervisory Authority to include the processing of location data in its list, together with another criterion.

EXCEPTIONS TO INFORMATION TO BE PROVIDED TO THE DATA SUBJECT ACCORDING TO ARTICLE 14.5 GDPR

The Board is of the opinion that types of processing activities that could deprive the data subjects from their rights do not represent a high risk on their own. Therefore, a processing activity conducted by the controller under article 14 GDPR and where the information to be given to the data subjects is subject to an exemption under article 14.5 (b)-(d) could require a DPIA to be carried out only in conjunction with at least one other criterion. The list submitted by the Finnish Supervisory Authority for an opinion of the Board does currently require a DPIA to be done for the processing of data where article 14(5), para (b) applies on its own. The Board requests the Finnish Supervisory Authority to amend its list accordingly, by adapting the list entry by adding that it requires a DPIA only in conjunction with at least one other criterion.

3. Conclusions / Recommendations

The draft list of the Finnish Supervisory Authority may lead to an inconsistent application of the requirement for a DPIA and the following changes need to made:

- Regarding the indicative nature of the list: the Board requests an explanation to be added to the document containing the list, stating its non-exhaustive nature.
- Regarding the reference to the guidelines: the Board requests the Finnish Supervisory Authority to amend its document accordingly.
- Regarding biometric data: the Board requests the Finnish Supervisory Authority to amend its list accordingly, by adding explicitly the processing of biometric data for the purpose of uniquely identifying a natural person in conjunction with at least one other criterion to its list.

- Regarding genetic data: the Board requests the Finnish Supervisory Authority to amend its list by adding that the item referencing the processing of genetic data requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.
- Regarding location data: the Board encourages the Finnish Supervisory Authority to include the processing of location data in its list, together with another criterion.
- Regarding the exceptions to the information to be given to the data subjects according to article 14.5 GDPR: the Board requests the Finnish Supervisory Authority to amend its list by adding that it requires a DPIA only in conjunction with at least one other criterion.

4. Final Remarks

This opinion is addressed to the Tietosuojavaltuutetun toimisto (Finnish Supervisory Authority) and will be made public pursuant to Article 64 (5b) GDPR.

According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 9/2018

on the draft list of the competent supervisory authority of France

regarding

**the processing operations subject to the requirement of a data protection
impact assessment (Article 35.4 GDPR)**

Adopted on 25th September 2018

Contents

1.	Summary of the Facts	4
2.	Assessment	5
2.1	General reasoning of the EDPB regarding the submitted list	5
2.2	Application of the consistency mechanism to the draft list	6
2.3	Analysis of the draft list.....	6
	Indicative nature of the list.....	6
	Reference to the Guidelines	6
	Biometric data.....	6
	Genetic data.....	7
	Location data	7
	Employee monitoring	7
3.	Conclusions / Recommendations	7
4.	Final Remarks.....	8

The European Data Protection Board

Having regard to Article 63, Article 64 (1a), (3) - (8) and Article 35 (1), (3), (4), (6) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (here after GDPR) throughout the European Economic Area. In compliance with article 64.1 GDPR, the Board has to issue an opinion where a supervisory authority intends to adopt a list of processing operations subject to the requirement for a data protection impact assessment pursuant to article 35.4 GDPR. The aim of this opinion is therefore to create a harmonized approach with regard to processing that is cross border or that can affect the free flow of personal data or natural person across the European Union. Even though the GDPR doesn't impose a single list, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by requesting SAs to include some types of processing in their lists, secondly by requesting them to remove some criteria which the Board doesn't consider as necessarily creating high risks for data subjects, and finally by requesting them to use some criteria in a harmonized manner.

(2) With reference to Article 35 (4) and (6) GDPR, the competent supervisory authorities shall establish lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment (hereinafter "DPIA"). They shall, however, apply the consistency mechanism where such lists involve processing operations, which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

(3) While the draft lists of the competent supervisory authorities are subject to the consistency mechanism, this does not mean that the lists should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB assessment/opinion is not to reach a single EU list but rather to avoid significant inconsistencies that may affect the equivalent protection of the data subjects.

(4) The carrying out of a DPIA is only mandatory for the controller pursuant to Article 35 (1) GDPR where processing is "likely to result in a high risk to the rights and freedoms of natural

persons". Article 35 (3) GDPR illustrates what is likely to result in a high risk. This is a non-exhaustive list. The Working Party 29 in the Guidelines on data protection impact assessment¹, as endorsed by the EDPB², has clarified criteria that can help to identify when processing operations are subject to the requirement for a DPIA. The Working Party 29 Guidelines

WP248 state that in most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out, however, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

(5) The lists produced by the competent supervisory authorities support the same objective to identify processing operations likely to result in a high risk and processing operations, which therefore require a DPIA. As such, the criteria developed in the Working Party 29 Guidelines should be applied when assessing whether the draft lists of the competent supervisory authorities does not affect the consistent application of the GDPR.

(6) Twenty-two competent supervisory authorities have submitted their draft lists to the EDPB. A global assessment of these draft lists supports the objective of a consistent application of the GDPR even though the complexity of the subject matter increases.

(7) The opinion of the EDPB shall be adopted pursuant to Article 64 (3) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

I. Summary of the Facts

The Commission Nationale de l'Informatique et des Libertés (hereafter French Supervisory Authority) has submitted its draft list to the EDPB. The decision on the completeness of the file was taken on the 9th of July. This period until which the opinion to be adopted has been extended until the 25th of September taking into account the complexity of the subject matter considering that at the same time twenty-two competent supervisory authorities submitted the draft lists and thus the need for a global assessment arose.

¹ WP29, Guidelines on Data Protection Impact Assessment and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP 248 rev. 01).

² EDPB, Endorsement 1/2018.

2. Assessment

2.1 General reasoning of the EDPB regarding the submitted list

Any list submitted to the EDPB has been interpreted as further specifying Art 35.1, which will prevail in any case. Thus, no list can be exhaustive. As the list provided by French Supervisory Authority does not explicitly state this, the Board requests this explanation to be added to the document containing the list.

In compliance with article 35.10 GDPR, the Board is of the opinion that if a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of the legal basis the obligation to carry out a DPIA in accordance with paragraphs 1 to 7 of article 35 GDPR does not apply, unless the Member State deems it necessary.

Further, if the Board requests a DPIA for a certain category of processing and an equivalent measure is already required by national law, the French Supervisory Authority shall add a reference to this measure.

This opinion does not reflect upon items submitted by the Commission Nationale de l’Informatique et des Libertés (French Supervisory Authority), which were deemed outside the scope of Article 35.6 GDPR. This refers to items that neither relate “to the offering of goods or services to data subjects” in several Member States nor to the monitoring of the behaviour of data subjects in several Member States. Additionally, they are not likely to “substantially affect the free movement of personal data within the Union”. This is especially the case for items relating to national legislation and in particular where the obligation to carry out a DPIA is stipulated in national legislation. Further, any processing operations that relate to law enforcement were deemed out of scope, as they are not in scope of the GDPR.

The Board has noted that several supervisory authorities have included in their lists some types of processing which are necessarily local processing. Given that only cross border processing and processing that may affect the free flow of personal data and data subjects are concerned by Article 35.6, the Board will not comment on those local processing.

The opinion aims at defining a consistent core of processing operations that are recurrent in the lists provided by the SAs.

This means that, for a limited number of types of processing operations, that will be defined in a harmonised way, all the Supervisory Authorities will require a DPIA to be carried out and the Board will recommend the SAs to amend their lists accordingly in order to ensure consistency.

When this opinion remains silent on DPIA list entries submitted, it means that the Board is not asking the French Supervisory Authority to take further action.

Finally, the Board recalls that transparency is key for data controllers and data processors. In order to clarify the entries in the list, the Board is of the opinion that making an explicit reference in the lists, for each type of processing, to the criteria set out in the guidelines could

improve this transparency. Therefore, the Board considers that an explanation on which criteria have been taken into account by the French Supervisory Authority to create its list could be added.

2.2 Application of the consistency mechanism to the draft list

The submitted draft list by the French Supervisory Authority relates to the offering of goods or services to data subjects, relates to the monitoring of their behaviour in several Member States and/or may substantially affect the free movement of personal data within the Union mainly because the processing operations in the submitted draft list are not limited to data subjects in this country.

2.3 Analysis of the draft list

Taking into account that:

- a. Article 35 (1) GDPR requires a DPIA when the processing activity is likely to result in a high risk to the rights and freedoms of natural persons; and
- b. Article 35 (3) GDPR provides a non-exhaustive list of types of processing that require a DPIA,

the Board is of the opinion that:

INDICATIVE NATURE OF THE LIST

As the list provided by French Supervisory Authority does not explicitly state that its list is not exhaustive, the Board requests this explanation to be added to the document containing the list.

REFERENCE TO THE GUIDELINES

The board is of the opinion that the analysis done in the Working Party 29 Guidelines WP248 are a core element for ensuring consistency across the Union. Thus, it requests the different Supervisor Authorities to add a statement to the document containing their list that clarifies that their list is based on these guidelines and that it complements and further specifies the guidelines.

As the document of the French Supervisory Authority does not contain such a statement, the Board recommends the French Supervisory Authority to amend its document accordingly.

BIOMETRIC DATA

The list submitted by the French Supervisory Authority for an opinion of the Board states, that the processing of biometric data falls under the obligation to perform a DPIA on its own. The Board is of the opinion that the processing of biometric data on its own is not necessarily likely to represent a high risk. However, the processing of biometric data for the purpose of uniquely identifying a natural person in conjunction with at least one other criterion requires a DPIA to be carried out. As such, the Board requests the French Supervisory Authority to amend its list accordingly, by adding that the item referencing the processing of biometric data for the purpose of uniquely identifying a natural person requires a DPIA to be carried out

only when it is done in conjunction of at least one other criterion , to be applied without prejudice to article 35(3) GDPR.

GENETIC DATA

The list submitted by the French Supervisory Authority for an opinion of the Board states, that the processing of genetic data falls under the obligation to perform a DPIA on its own. The Board is of the opinion that the processing of genetic data on its own is not necessarily likely to represent a high risk. However, the processing of genetic data in conjunction with at least one other criterion requires a DPIA to be carried out. As such, the Board requests the French Supervisory Authority to amend its list accordingly, by adding that the item referencing the processing of genetic data requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion, to be applied without prejudice to article 35(3) GDPR.

LOCATION DATA

The Board is of the opinion that consistency is one of the basic principle of the GDPR. The Board notes that a majority of the lists submitted explicitly contain a reference to the processing of location data. As the list submitted by the French Supervisory Authority for an opinion do not contain such a reference, the Board encourages the French Supervisory Authority to include the processing of location data in its list, together with another criterion.

EMPLOYEE MONITORING

The Board is of the opinion that, due to its specific nature, the employee monitoring processing, meeting the criterion of vulnerable data subjects and of systematic monitoring in the guidelines, – could require a DPIA. Given that the list submitted by the French Supervisory Authority for an opinion of the Board already envisages this type of processing as requiring a data protection impact assessment, the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248. In addition, the Board is of the opinion that the WP249 of the Article 29 working party remains valid when defining the concept of the systematic processing of employee data.

3. Conclusions / Recommendations

The draft list of the French Supervisory Authority may lead to an inconsistent application of the requirement for a DPIA and the following changes need to made:

- Regarding the indicative nature of the list: the Board requests an explanation to be added to the document containing the list, stating its non-exhaustive nature.
- Regarding the reference to the guidelines: the Board requests the French Supervisory Authority to amend its document accordingly.
- Regarding biometric data: the Board requests the French Supervisory Authority to amend its list by adding that the item referencing the processing of biometric data for the purpose of uniquely identifying a natural person requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion

- Regarding genetic data: the Board requests the French Supervisory Authority to amend its list by adding that the item referencing the processing of genetic data requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.
- Regarding location data: the Board encourages the French Supervisory Authority to include the processing of location data in its list, together with another criterion.
- Regarding employment monitoring: the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248. w

4. Final Remarks

This opinion is addressed to the Commission Nationale de l'Informatique et des Libertés (French Supervisory Authority) and will be made public pursuant to Article 64 (5b) GDPR.

According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 7/2018

on the draft list of the competent supervisory authority of Greece

regarding

**the processing operations subject to the requirement of a data protection
impact assessment (Article 35.4 GDPR)**

Adopted on 25th September 2018

Contents

1.	Summary of the Facts	4
2.	Assessment	5
2.1	General reasoning of the EDPB regarding the submitted list	5
2.2	Application of the consistency mechanism to the draft list	6
2.3	Analysis of the draft list.....	6
	Reference to the Guidelines	6
	Biometric data.....	6
	Genetic data.....	6
	Large scale.....	7
	Processing for scientific or historical purposes without consent	7
	Exceptions to information to be provided to the data subject according to article 14.5 GDPR	7
	Processing carried out with the aid of an implant.....	7
3.	Conclusions / Recommendations	7
4.	Final Remarks.....	8

The European Data Protection Board

Having regard to Article 63, Article 64 (1a), (3) - (8) and Article 35 (1), (3), (4), (6) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (here after GDPR) throughout the European Economic Area. In compliance with article 64.1 GDPR, the Board has to issue an opinion where a supervisory authority intends to adopt a list of processing operations subject to the requirement for a data protection impact assessment pursuant to article 35.4 GDPR. The aim of this opinion is therefore to create a harmonized approach with regard to processing that is cross border or that can affect the free flow of personal data or natural person across the European Union. Even though the GDPR doesn't impose a single list, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by requesting SAs to include some types of processing in their lists, secondly by requesting them to remove some criteria which the Board doesn't consider as necessarily creating high risks for data subjects, and finally by requesting them to use some criteria in a harmonized manner.

(2) With reference to Article 35 (4) and (6) GDPR, the competent supervisory authorities shall establish lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment (hereinafter "DPIA"). They shall, however, apply the consistency mechanism where such lists involve processing operations, which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

(3) While the draft lists of the competent supervisory authorities are subject to the consistency mechanism, this does not mean that the lists should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB assessment/opinion is not to reach a single EU list but rather to avoid significant inconsistencies that may affect the equivalent protection of the data subjects.

(4) The carrying out of a DPIA is only mandatory for the controller pursuant to Article 35 (1) GDPR where processing is "likely to result in a high risk to the rights and freedoms of natural

persons". Article 35 (3) GDPR illustrates what is likely to result in a high risk. This is a non-exhaustive list. The Working Party 29 in the Guidelines on data protection impact assessment¹, as endorsed by the EDPB², has clarified criteria that can help to identify when processing operations are subject to the requirement for a DPIA. The Working Party 29 Guidelines WP248 state that in most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out, however, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

(5) The lists produced by the competent supervisory authorities support the same objective to identify processing operations likely to result in a high risk and processing operations, which therefore require a DPIA. As such, the criteria developed in the Working Party 29 Guidelines should be applied when assessing whether the draft lists of the competent supervisory authorities does not affect the consistent application of the GDPR.

(6) Twenty-two competent supervisory authorities have submitted their draft lists to the EDPB. A global assessment of these draft lists supports the objective of a consistent application of the GDPR even though the complexity of the subject matter increases.

(7) The opinion of the EDPB shall be adopted pursuant to Article 64 (3) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

I. Summary of the Facts

The Hellenic Data Protection Authority (hereafter Greek Supervisory Authority) has submitted its draft list to the EDPB. The decision on the completeness of the file was taken on 10th July 2018. This period until which the opinion to be adopted has been extended until the 25th of September taking into account the complexity of the subject matter considering that at the same time twenty-two competent supervisory authorities submitted the draft lists and thus the need for a global assessment arose.

¹ WP29, Guidelines on Data Protection Impact Assessment and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP 248 rev. 01).

² EDPB, Endorsement 1/2018.

2. Assessment

2.1 General reasoning of the EDPB regarding the submitted list

Any list submitted to the EDPB has been interpreted as further specifying Art 35.1, which will prevail in any case. Thus, no list can be exhaustive.

In compliance with article 35.10 GDPR, the Board is of the opinion that if a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of the legal basis the obligation to carry out a DPIA in accordance with paragraphs 1 to 7 of article 35 GDPR does not apply, unless the Member State deems it necessary.

Further, if the Board requests a DPIA for a certain category of processing and an equivalent measure is already required by national law, the Greek Supervisory Authority shall add a reference to this measure.

This opinion does not reflect upon items submitted by the Greek Supervisory Authority, which were deemed outside the scope of Article 35.6 GDPR. This refers to items that neither relate "to the offering of goods or services to data subjects" in several Member States nor to the monitoring of the behaviour of data subjects in several Member States. Additionally, they are not likely to "substantially affect the free movement of personal data within the Union". This is especially the case for items relating to national legislation and in particular where the obligation to carry out a DPIA is stipulated in national legislation. Further, any processing operations that relate to law enforcement were deemed out of scope, as they are not in scope of the GDPR.

The Board has noted that several supervisory authorities have included in their lists some types of processing which are necessarily local processing. Given that only cross border processing and processing that may affect the free flow of personal data and data subjects are concerned by Article 35.6, the Board will not comment on those local processing.

The opinion aims at defining a consistent core of processing operations that are recurrent in the lists provided by the SAs.

This means that, for a limited number of types of processing operations, that will be defined in a harmonised way, all the Supervisory Authorities will require a DPIA to be carried out and the Board will recommend the SAs to amend their lists accordingly in order to ensure consistency.

When this opinion remains silent on DPIA list entries submitted, it means that the Board is not asking the Greek Supervisory Authority to take further action.

Finally, the Board recalls that transparency is key for data controllers and data processors. In order to clarify the entries in the list, the Board is of the opinion that making an explicit reference in the lists, for each type of processing, to the criteria set out in the guidelines could improve this transparency. Therefore, the Board considers that an explanation on which

criteria have been taken into account by the Greek Supervisory Authority to create its list could be added.

2.2 Application of the consistency mechanism to the draft list

The submitted draft list by the Greek Supervisory Authority relates to the offering of goods or services to data subjects, relates to the monitoring of their behaviour in several Member States and/or may substantially affect the free movement of personal data within the Union mainly because the processing operations in the submitted draft list are not limited to data subjects in this country.

2.3 Analysis of the draft list

Taking into account that:

- a. Article 35 (1) GDPR requires a DPIA when the processing activity is likely to result in a high risk to the rights and freedoms of natural persons; and
- b. Article 35 (3) GDPR provides a non-exhaustive list of types of processing that require a DPIA,

the Board is of the opinion that:

REFERENCE TO THE GUIDELINES

The board is of the opinion that the analysis done in the Working Party 29 Guidelines WP248 are a core element for ensuring consistency across the Union. Thus, it requests the different Supervisor Authorities to add a statement to the document containing their list that clarifies that their list is based on these guidelines and that it complements and further specifies the guidelines.

As the document of the Greek Supervisory Authority does not contain such a statement, the Board recommends the Greek Supervisory Authority to amend its document accordingly.

BIOMETRIC DATA

The list submitted by the Greek Supervisory Authority for an opinion of the Board envisages that the processing of biometric data for the purpose of uniquely identifying a natural person, in conjunction with at least one other criterion, requires a DPIA. On this point, the Board acknowledges that the list aligns with the aim of consistency.

GENETIC DATA

The list submitted by the Greek Supervisory Authority for an opinion of the Board envisages that the processing of genetic data, in conjunction with at least one other criterion, requires a DPIA. The Board is of the opinion that the processing of genetic data on its own is not necessarily likely to represent a high risk. However, the processing of genetic data in conjunction with at least one other criterion requires a DPIA to be carried out. The Board takes note of the inclusion of this criterion in the list of Greek Supervisory Authority.

LARGE SCALE

The GDPR does not precisely define what constitutes large-scale. In the WP29 guidelines on Data Protection Officer and on DPIA, both endorsed by Board, it has recommended to take in account several specific factors when determining whether a processing is carried out on a large scale.

The Board is of the opinion that those factors are sufficient to assess whether the processing of personal data is undertaken on a large scale. Therefore the Board requests the Greek Supervisory Authority to amend its list accordingly, by deleting the explicit figures in its list, and making reference to the previously mentioned definitions of large scale.

PROCESSING FOR SCIENTIFIC OR HISTORICAL PURPOSES WITHOUT CONSENT

The Board is of the opinion that the processing of personal data for scientific or historical purposes on its own is not necessarily likely to represent a high risk. However, the processing of personal data for scientific or historical purpose in conjunction with at least one other criterion does require a DPIA to be carried out. The list submitted by the Greek Supervisory Authority for an opinion of the Board states that this type of processing in conjunction with at least one other criterion falls under the obligation to perform a DPIA. The Board takes note of the inclusion of this criterion in the list.

EXCEPTIONS TO INFORMATION TO BE PROVIDED TO THE DATA SUBJECT ACCORDING TO ARTICLE 14.5 GDPR

The Board is of the opinion that types of processing activities that could deprive the data subjects from their rights do not represent a high risk on their own. Therefore, a processing activity conducted by the controller under article 14 GDPR and where the information to be given to the data subjects is subject to an exemption under article 14.5 (b)-(d) could require a DPIA to be carried out only in conjunction with at least one other criterion. The list submitted by the Greek Supervisory Authority for an opinion of the Board states that this type of processing in conjunction with at least one other criterion falls under the obligation to perform a DPIA. The Board takes note of the inclusion of this criterion in the list.

PROCESSING CARRIED OUT WITH THE AID OF AN IMPLANT

The Board is of the opinion that, the processing of non-health data with the aid of an implant does not require a DPIA in every instance. The list submitted by the Greek Supervisory Authority for an opinion of the Board does currently not clarify that a DPIA is to be done for the processing of health data with the aid of an implant. As such, the Board requests the Greek Supervisory Authority to amend its list accordingly, by stating that in any event the processing of health data with the aid of an implant requires a DPIA to be carried out.

3. Conclusions / Recommendations

The draft list of the Greek Supervisory Authority may lead to an inconsistent application of the requirement for a DPIA and the following changes need to made:

- Regarding the reference to the guidelines: the Board requests the Greek Supervisory Authority to amend its document accordingly.
- Regarding the notion of large scale: the Board requests the Greek Supervisory Authority to amend its list by deleting the explicit figures in its list, and making reference to the definitions of large scale mentioned in the WP29 guidelines on Data Protection Officer (WP243) and on DPIA (WP248).
- Regarding processing carried out with the aid of an implant: the Board requests the Greek Supervisory Authority to amend its list by stating that only the processing of health data with the aid of an implant requires a DPIA to be carried out.

4. Final Remarks

This opinion is addressed to the Hellenic Data Protection Authority (Greek Supervisory Authority) and will be made public pursuant to Article 64 (5b) GDPR.

According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 10/2018

on the draft list of the competent supervisory authority of Hungary

regarding

**the processing operations subject to the requirement of a data protection
impact assessment (Article 35.4 GDPR)**

Adopted on 25th September 2018

Contents

1.	Summary of the Facts	4
2.	Assessment	5
2.1	General reasoning of the EDPB regarding the submitted list	5
2.2	Application of the consistency mechanism to the draft list	6
2.3	Analysis of the draft list.....	6
	Reference to the Guidelines	6
	Biometric data.....	6
	Genetic data.....	7
	Biometric ‘and’ genetic data.....	7
	Location data	7
	Data collected via third parties (article 19 GDPR)	7
	Employee Monitoring	8
	Processing using new/innovative technology	8
3.	Conclusions / Recommendations	8
4.	Final Remarks	9

The European Data Protection Board

Having regard to Article 63, Article 64 (1a), (3) - (8) and Article 35 (1), (3), (4), (6) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (here after GDPR) throughout the European Economic Area. In compliance with article 64.1 GDPR, the Board has to issue an opinion where a supervisory authority intends to adopt a list of processing operations subject to the requirement for a data protection impact assessment pursuant to article 35.4 GDPR. The aim of this opinion is therefore to create a harmonized approach with regard to processing that is cross border or that can affect the free flow of personal data or natural person across the European Union. Even though the GDPR doesn't impose a single list, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by requesting SAs to include some types of processing in their lists, secondly by requesting them to remove some criteria which the Board doesn't consider as necessarily creating high risks for data subjects, and finally by requesting them to use some criteria in a harmonized manner.

(2) With reference to Article 35 (4) and (6) GDPR, the competent supervisory authorities shall establish lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment (hereinafter "DPIA"). They shall, however, apply the consistency mechanism where such lists involve processing operations, which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

(3) While the draft lists of the competent supervisory authorities are subject to the consistency mechanism, this does not mean that the lists should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB assessment/opinion is not to reach a single EU list but rather to avoid significant inconsistencies that may affect the equivalent protection of the data subjects.

(4) The carrying out of a DPIA is only mandatory for the controller pursuant to Article 35 (1) GDPR where processing is "likely to result in a high risk to the rights and freedoms of natural

persons". Article 35 (3) GDPR illustrates what is likely to result in a high risk. This is a non-exhaustive list. The Working Party 29 in the Guidelines on data protection impact assessment¹, as endorsed by the EDPB², has clarified criteria that can help to identify when processing operations are subject to the requirement for a DPIA. The Working Party 29 Guidelines WP248 state that in most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out, however, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

(5) The lists produced by the competent supervisory authorities support the same objective to identify processing operations likely to result in a high risk and processing operations, which therefore require a DPIA. As such, the criteria developed in the Working Party 29 Guidelines should be applied when assessing whether the draft lists of the competent supervisory authorities does not affect the consistent application of the GDPR.

(6) Twenty-two competent supervisory authorities have submitted their draft lists to the EDPB. A global assessment of these draft lists supports the objective of a consistent application of the GDPR even though the complexity of the subject matter increases.

(7) The opinion of the EDPB shall be adopted pursuant to Article 64 (3) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

I. Summary of the Facts

The Nemzeti Adatvédelmi és Információszabadság Hatóság (hereafter Hungarian Supervisory Authority) has submitted its draft list to the EDPB. The decision on the completeness of the file was taken on the 27th of June 2018. This period until which the opinion to be adopted has been extended until the 25th of September taking into account the complexity of the subject matter considering that at the same time twenty-two competent supervisory authorities submitted the draft lists and thus the need for a global assessment arose.

¹ WP29, Guidelines on Data Protection Impact Assessment and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP 248 rev. 01).

² EDPB, Endorsement 1/2018.

2. Assessment

2.1 General reasoning of the EDPB regarding the submitted list

Any list submitted to the EDPB has been interpreted as further specifying Art 35.1, which will prevail in any case. Thus, no list can be exhaustive.

In compliance with article 35.10 GDPR, the Board is of the opinion that if a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of the legal basis the obligation to carry out a DPIA in accordance with paragraphs 1 to 7 of article 35 GDPR does not apply, unless the Member State deems it necessary.

Further, if the Board requests a DPIA for a certain category of processing and an equivalent measure is already required by national law, the Hungarian Supervisory Authority shall add a reference to this measure.

This opinion does not reflect upon items submitted by the Hungarian Supervisory Authority, which were deemed outside the scope of Article 35.6 GDPR. This refers to items that neither relate “to the offering of goods or services to data subjects” in several Member States nor to the monitoring of the behaviour of data subjects in several Member States. Additionally, they are not likely to “substantially affect the free movement of personal data within the Union”. This is especially the case for items relating to national legislation and in particular where the obligation to carry out a DPIA is stipulated in national legislation. Further, any processing operations that relate to law enforcement were deemed out of scope, as they are not in scope of the GDPR.

The Board has noted that several supervisory authorities have included in their lists some types of processing which are necessarily local processing. Given that only cross border processing and processing that may affect the free flow of personal data and data subjects are concerned by Article 35.6, the Board will not comment on those local processing.

The opinion aims at defining a consistent core of processing operations that are recurrent in the lists provided by the SAs.

This means that, for a limited number of types of processing operations, that will be defined in a harmonised way, all the Supervisory Authorities will require a DPIA to be carried out and the Board will recommend the SAs to amend their lists accordingly in order to ensure consistency.

When this opinion remains silent on DPIA list entries submitted, it means that the Board is not asking the Hungarian Supervisory Authority to take further action.

Finally, the Board recalls that transparency is key for data controllers and data processors. In order to clarify the entries in the list, the Board is of the opinion that making an explicit reference in the lists, for each type of processing, to the criteria set out in the guidelines could improve this transparency. Therefore, the Board considers that an explanation on which

criteria have been taken into account by the Hungarian Supervisory Authority to create its list could be added.

2.2 Application of the consistency mechanism to the draft list

The submitted draft list by the Hungarian Supervisory Authority relates to the offering of goods or services to data subjects, relates to the monitoring of their behaviour in several Member States and/or may substantially affect the free movement of personal data within the Union mainly because the processing operations in the submitted draft list are not limited to data subjects in this country.

2.3 Analysis of the draft list

Taking into account that:

- a. Article 35 (1) GDPR requires a DPIA when the processing activity is likely to result in a high risk to the rights and freedoms of natural persons; and
- b. Article 35 (3) GDPR provides a non-exhaustive list of types of processing that require a DPIA,

the Board is of the opinion that:

REFERENCE TO THE GUIDELINES

The board is of the opinion that the analysis done in the Working Party 29 Guidelines WP248 are a core element for ensuring consistency across the Union. Thus, it requests the different Supervisor Authorities to add a statement to the document containing their list that clarifies that their list is based on these guidelines and that it complements and further specifies the guidelines.

As the document of the Hungarian Supervisory Authority does not contain such a statement, the Board recommends the Hungarian Supervisory Authority to amend its document accordingly.

BIOMETRIC DATA

The list submitted by the Hungarian Supervisory Authority for an opinion of the Board states, that the processing of biometric data falls under the obligation to perform a DPIA on its own. The Board is of the opinion that the processing of biometric data on its own is not necessarily likely to represent a high risk. However, the processing of biometric data for the purpose of uniquely identifying a natural person in conjunction with at least one other criterion requires a DPIA to be carried out. As such, the Board requests the Hungarian Supervisory Authority to amend its list accordingly, by adding that the item referencing the processing of biometric data for the purpose of uniquely identifying a natural person requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion, to be applied without prejudice to article 35(3) GDPR.

GENETIC DATA

The list submitted by the Hungarian Supervisory Authority for an opinion of the Board states, that the processing of genetic data falls under the obligation to perform a DPIA on its own. The Board is of the opinion that the processing of genetic data on its own is not necessarily likely to represent a high risk. However, the processing of genetic data in conjunction with at least one other criterion requires a DPIA to be carried out. As such, the Board requests the Hungarian Supervisory Authority to amend its list accordingly, by adding that the item referencing the processing of genetic data requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion, to be applied without prejudice to article 35(3) GDPR.

BIOMETRIC 'AND' GENETIC DATA

The list submitted by the Hungarian Supervisory Authority for an opinion includes a reference to biometric and genetic data (cumulatively) as a separate entry. The Board has been informed by the Hungarian Supervisory Authority that in the original language version biometric and genetic data are in fact considered separately. Therefore, the Board refers to the sections in the opinion on biometric data and genetic data respectively.

LOCATION DATA

The Board is of the opinion that consistency is one of the basic principle of the GDPR. The Board notes that a majority of the lists submitted explicitly contain a reference to the processing of location data. As the list submitted by the Hungarian Supervisory Authority for an opinion do not contain such a reference, the Board encourages the Hungarian Supervisory Authority to include the processing of location data in its list, together with another criterion.

DATA COLLECTED VIA THIRD PARTIES (ARTICLE 19 GDPR)

The Board is of the opinion that types of processing activities that could deprive the data subjects from their rights on their own do not represent a high risk. Further, the Board is of the opinion that a processing activity conducted by the controller under article 19 GDPR and where the information of recipients would prove impossible or require a disproportionate effort only requires a DPIA to be carried out when this processing involves at least one other criterion. The list submitted by the Hungarian Supervisory Authority for an opinion of the Board states that this type of processing on its own falls under the obligation to perform a DPIA. The Board requests the Hungarian Supervisory Authority to amend its list accordingly, by adding that the item referencing the processing of personal data collected via third parties requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.

EMPLOYEE MONITORING

The Board is of the opinion that, due to its specific nature, the employee monitoring processing, meeting the criterion of vulnerable data subjects and of systematic monitoring in the guidelines, – could require a DPIA. Given that the list submitted by the Hungarian Supervisory Authority for an opinion of the Board already envisages this type of processing as requiring a data protection impact assessment, the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248. In addition, the Board is of the opinion that the WP249 of the Article 29 working party remains valid when defining the concept of the systematic processing of employee data.

PROCESSING USING NEW/INNOVATIVE TECHNOLOGY

The list submitted by the Hungarian Supervisory Authority for an opinion of the Board envisages that the processing of personal data using innovative technology in conjunction with at least one other criterion, requires a DPIA. The Board takes note of the inclusion of this criterion in the list.

3. Conclusions / Recommendations

The draft list of the Hungarian Supervisory Authority may lead to an inconsistent application of the requirement for a DPIA and the following changes need to made:

- Regarding the reference to the guidelines: the Board requests the Hungarian Supervisory Authority to amend its document accordingly.
- Regarding biometric data: the Board requests the Hungarian Supervisory Authority to amend its list by adding that the item referencing the processing of biometric data for the purpose of uniquely identifying a natural person requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion
- Regarding genetic data: the Board requests the Hungarian Supervisory Authority to amend its list by adding that the item referencing the processing of genetic data requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.
- Regarding location data: the Board encourages the Hungarian Supervisory Authority to include the processing of location data in its list, together with another criterion.
- Regarding the data collected via third parties (article 19 GDPR): the Board requests the Hungarian Supervisory Authority to amend its list by adding that the item referencing the processing of personal data collected via third parties requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.
- Regarding employment monitoring: the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248.

4. Final Remarks

This opinion is addressed to the Nemzeti Adatvédelmi és Információszabadság Hatóság (Hungarian Supervisory Authority) and will be made public pursuant to Article 64 (5b) GDPR.

According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 11/2018

on the draft list of the competent supervisory authority of Ireland

regarding

**the processing operations subject to the requirement of a data protection
impact assessment (Article 35.4 GDPR)**

Adopted on 25th September 2018

Contents

1.	Summary of the Facts	4
2.	Assessment	5
2.1	General reasoning of the EDPB regarding the submitted list	5
2.2	Application of the consistency mechanism to the draft list	6
2.3	Analysis of the draft list.....	6
	Indicative nature of the list.....	6
	Reference to the Guidelines	6
	Biometric data.....	6
	Genetic data.....	7
	Location data	7
	Processing for scientific or historical purposes without consent.....	7
	Further processing	7
	Employee Monitoring	7
3.	Conclusions / Recommendations	8
4.	Final Remarks	9

The European Data Protection Board

Having regard to Article 63, Article 64 (1a), (3) - (8) and Article 35 (1), (3), (4), (6) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (here after GDPR) throughout the European Economic Area. In compliance with article 64.1 GDPR, the Board has to issue an opinion where a supervisory authority intends to adopt a list of processing operations subject to the requirement for a data protection impact assessment pursuant to article 35.4 GDPR. The aim of this opinion is therefore to create a harmonized approach with regard to processing that is cross border or that can affect the free flow of personal data or natural person across the European Union. Even though the GDPR doesn't impose a single list, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by requesting SAs to include some types of processing in their lists, secondly by requesting them to remove some criteria which the Board doesn't consider as necessarily creating high risks for data subjects, and finally by requesting them to use some criteria in a harmonized manner.

(2) With reference to Article 35 (4) and (6) GDPR, the competent supervisory authorities shall establish lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment (hereinafter "DPIA"). They shall, however, apply the consistency mechanism where such lists involve processing operations, which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

(3) While the draft lists of the competent supervisory authorities are subject to the consistency mechanism, this does not mean that the lists should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB assessment/opinion is not to reach a single EU list but rather to avoid significant inconsistencies that may affect the equivalent protection of the data subjects.

(4) The carrying out of a DPIA is only mandatory for the controller pursuant to Article 35 (1) GDPR where processing is "likely to result in a high risk to the rights and freedoms of natural

persons". Article 35 (3) GDPR illustrates what is likely to result in a high risk. This is a non-exhaustive list. The Working Party 29 in the Guidelines on data protection impact assessment¹, as endorsed by the EDPB², has clarified criteria that can help to identify when processing operations are subject to the requirement for a DPIA. The Working Party 29 Guidelines WP248 state that in most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out, however, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

(5) The lists produced by the competent supervisory authorities support the same objective to identify processing operations likely to result in a high risk and processing operations, which therefore require a DPIA. As such, the criteria developed in the Working Party 29 Guidelines should be applied when assessing whether the draft lists of the competent supervisory authorities does not affect the consistent application of the GDPR.

(6) Twenty-two competent supervisory authorities have submitted their draft lists to the EDPB. A global assessment of these draft lists supports the objective of a consistent application of the GDPR even though the complexity of the subject matter increases.

(7) The opinion of the EDPB shall be adopted pursuant to Article 64 (3) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

I. Summary of the Facts

The Data Protection Commission (hereafter Irish Supervisory Authority) has submitted its draft list to the EDPB. The decision on the completeness of the file was taken on the 11th of July 2018. This period until which the opinion to be adopted has been extended until the 25th of September taking into account the complexity of the subject matter considering that at the same time twenty-two competent supervisory authorities submitted the draft lists and thus the need for a global assessment arose.

¹ WP29, Guidelines on Data Protection Impact Assessment and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP 248 rev. 01).

² EDPB, Endorsement 1/2018.

2. Assessment

2.1 General reasoning of the EDPB regarding the submitted list

Any list submitted to the EDPB has been interpreted as further specifying Art 35.1, which will prevail in any case. Thus, no list can be exhaustive. As the list provided by Irish Supervisory Authority does not explicitly state this, the Board requests this explanation to be added to the document containing the list.

In compliance with article 35.10 GDPR, the Board is of the opinion that if a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of the legal basis the obligation to carry out a DPIA in accordance with paragraphs 1 to 7 of article 35 GDPR does not apply, unless the Member State deems it necessary.

Further, if the Board requests a DPIA for a certain category of processing and an equivalent measure is already required by national law, the Irish Supervisory Authority shall add a reference to this measure.

This opinion does not reflect upon items submitted by the Irish Supervisory Authority, which were deemed outside the scope of Article 35.6 GDPR. This refers to items that neither relate "to the offering of goods or services to data subjects" in several Member States nor to the monitoring of the behaviour of data subjects in several Member States. Additionally, they are not likely to "substantially affect the free movement of personal data within the Union". This is especially the case for items relating to national legislation and in particular where the obligation to carry out a DPIA is stipulated in national legislation. Further, any processing operations that relate to law enforcement were deemed out of scope, as they are not in scope of the GDPR.

The Board has noted that several supervisory authorities have included in their lists some types of processing which are necessarily local processing. Given that only cross border processing and processing that may affect the free flow of personal data and data subjects are concerned by Article 35.6, the Board will not comment on those local processing.

The opinion aims at defining a consistent core of processing operations that are recurrent in the lists provided by the SAs.

This means that, for a limited number of types of processing operations, that will be defined in a harmonised way, all the Supervisory Authorities will require a DPIA to be carried out and the Board will recommend the SAs to amend their lists accordingly in order to ensure consistency.

When this opinion remains silent on DPIA list entries submitted, it means that the Board is not asking the Irish Supervisory Authority to take further action.

Finally, the Board recalls that transparency is key for data controllers and data processors. In order to clarify the entries in the list, the Board is of the opinion that making an explicit

reference in the lists, for each type of processing, to the criteria set out in the guidelines could improve this transparency. Therefore, the Board considers that an explanation on which criteria have been taken into account by the Irish Supervisory Authority to create its list could be added.

2.2 Application of the consistency mechanism to the draft list

The submitted draft list by the Irish Supervisory Authority relates to the offering of goods or services to data subjects, relates to the monitoring of their behaviour in several Member States and/or may substantially affect the free movement of personal data within the Union mainly because the processing operations in the submitted draft list are not limited to data subjects in this country.

2.3 Analysis of the draft list

Taking into account that:

- a. Article 35 (1) GDPR requires a DPIA when the processing activity is likely to result in a high risk to the rights and freedoms of natural persons; and
- b. Article 35 (3) GDPR provides a non-exhaustive list of types of processing that require a DPIA,

the Board is of the opinion that:

INDICATIVE NATURE OF THE LIST

As the list provided by Irish Supervisory Authority does not explicitly state that its list is not exhaustive, the Board requests this explanation to be added to the document containing the list.

REFERENCE TO THE GUIDELINES

The board is of the opinion that the analysis done in the Working Party 29 Guidelines WP248 are a core element for ensuring consistency across the Union. Thus, it requests the different Supervisor Authorities to add a statement to the document containing their list that clarifies that their list is based on these guidelines and that it complements and further specifies the guidelines.

As the document of the Irish Supervisory Authority does not contain such a statement, the Board recommends the Irish Supervisory Authority to amend its document accordingly.

BIOMETRIC DATA

The list submitted by the Irish Supervisory Authority for an opinion of the Board states, that the processing of biometric data falls under the obligation to perform a DPIA on its own. The Board is of the opinion that the processing of biometric data on its own is not necessarily likely to represent a high risk. However, the processing of biometric data for the purpose of uniquely identifying a natural person in conjunction with at least one other criterion requires a DPIA to be carried out. As such, the Board requests the Irish Supervisory Authority to amend its list accordingly, by adding that the item referencing the processing of biometric data for the purpose of uniquely identifying a natural person requires a DPIA to be carried out only

when it is done in conjunction of at least one other criterion, to be applied without prejudice to article 35(3) GDPR.

GENETIC DATA

The list submitted by the Irish Supervisory Authority for an opinion of the Board states, that the processing of genetic data falls under the obligation to perform a DPIA on its own. The Board is of the opinion that the processing of genetic data on its own is not necessarily likely to represent a high risk. However, the processing of genetic data in conjunction with at least one other criterion requires a DPIA to be carried out. As such, the Board requests the Irish Supervisory Authority to amend its list accordingly, by adding that the item referencing the processing of genetic data requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion, to be applied without prejudice to article 35(3) GDPR.

LOCATION DATA

The Board is of the opinion that the processing of location data on its own is not necessarily likely to represent a high risk. However, the processing of location data in conjunction with at least one other criterion requires a DPIA to be carried out. The list submitted by the Irish Supervisory Authority for an opinion of the Board does currently require a DPIA to be carried out when there is a processing of location data on its own. The Board requests the Irish Supervisory Authority to amend its list accordingly, by adding that the item referencing the processing of location data requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.

PROCESSING FOR SCIENTIFIC OR HISTORICAL PURPOSES WITHOUT CONSENT

The Board is of the opinion that the processing of personal data for scientific or historical purposes on its own is not necessarily likely to represent a high risk. However, the processing of personal data for scientific or historical purpose in conjunction with at least one other criterion does require a DPIA to be carried out. The list submitted by the Irish Supervisory Authority for an opinion of the Board states that this type of processing in conjunction with at least one other criterion falls under the obligation to perform a DPIA. The Board takes note of the inclusion of this criterion in the list.

FURTHER PROCESSING

The Board is of the opinion that further processing of personal data should not be a criterion leading to an obligation to do a DPIA, alone or with another criterion. The list submitted by the Irish Supervisory Authority for an opinion of the Board does currently require a DPIA to be carried out for the further processing of personal data. The Board requests the Irish Supervisory Authority to amend its list accordingly, by removing this criterion.

EMPLOYEE MONITORING

The Board is of the opinion that the systematic processing of vulnerable data subjects including that of employees meets two criteria in the guidelines and so could require a DPIA. Given that the list submitted by the Irish Supervisory Authority for an opinion of the Board already envisages this type of processing as requiring a data protection impact assessment,

the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248. In addition, the Board is of the opinion that the WP249 of the Article 29 working party remains valid when defining the concept of the systematic processing of employee data.

3. Conclusions / Recommendations

The draft list of the Irish Supervisory Authority may lead to an inconsistent application of the requirement for a DPIA and the following changes need to made:

- Regarding the indicative nature of the list: the Board requests an explanation to be added to the document containing the list, stating its non-exhaustive nature.
- Regarding the reference to the guidelines: the Board requests the Irish Supervisory Authority to amend its document accordingly.
- Regarding biometric data: the Board requests the Irish Supervisory Authority to amend its list by adding that the item referencing the processing of biometric data for the purpose of uniquely identifying a natural person requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion
- Regarding genetic data: the Board requests the Irish Supervisory Authority to amend its list by adding that the item referencing the processing of genetic data requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.
- Regarding location data: the Board requests the Irish Supervisory Authority to amend its list by adding that the item referencing the processing of location data requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.
- Regarding further processing: the Board requests the Irish Supervisory Authority to amend its list accordingly, by removing this criterion.
- Regarding employment monitoring: the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248.

4. Final Remarks

This opinion is addressed to the Data Protection Commission (Irish Supervisory Authority) and will be made public pursuant to Article 64 (5b) GDPR.

According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 12/2018

on the draft list of the competent supervisory authority of Italy

regarding

**the processing operations subject to the requirement of a data protection
impact assessment (Article 35.4 GDPR)**

Adopted on 25th September 2018

Contents

1.	Summary of the Facts	4
2.	Assessment	5
2.1	General reasoning of the EDPB regarding the submitted list	5
2.2	Application of the consistency mechanism to the draft list	6
2.3	Analysis of the draft list.....	6
	Indicative nature of the list.....	6
	Reference to the Guidelines	6
	Biometric data.....	6
	Genetic data.....	7
	Further processing	7
	Employee Monitoring	7
	Referencing a specific legal basis.....	7
	Processing using new/innovative technology	7
3.	Conclusions / Recommendations	8
4.	Final Remarks	9

The European Data Protection Board

Having regard to Article 63, Article 64 (1a), (3) - (8) and Article 35 (1), (3), (4), (6) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (here after GDPR) throughout the European Economic Area. In compliance with article 64.1 GDPR, the Board has to issue an opinion where a supervisory authority intends to adopt a list of processing operations subject to the requirement for a data protection impact assessment pursuant to article 35.4 GDPR. The aim of this opinion is therefore to create a harmonized approach with regard to processing that is cross border or that can affect the free flow of personal data or natural person across the European Union. Even though the GDPR doesn't impose a single list, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by requesting SAs to include some types of processing in their lists, secondly by requesting them to remove some criteria which the Board doesn't consider as necessarily creating high risks for data subjects, and finally by requesting them to use some criteria in a harmonized manner.

(2) With reference to Article 35 (4) and (6) GDPR, the competent supervisory authorities shall establish lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment (hereinafter "DPIA"). They shall, however, apply the consistency mechanism where such lists involve processing operations, which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

(3) While the draft lists of the competent supervisory authorities are subject to the consistency mechanism, this does not mean that the lists should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB assessment/opinion is not to reach a single EU list but rather to avoid significant inconsistencies that may affect the equivalent protection of the data subjects.

(4) The carrying out of a DPIA is only mandatory for the controller pursuant to Article 35 (1) GDPR where processing is "likely to result in a high risk to the rights and freedoms of natural

persons". Article 35 (3) GDPR illustrates what is likely to result in a high risk. This is a non-exhaustive list. The Working Party 29 in the Guidelines on data protection impact assessment¹, as endorsed by the EDPB², has clarified criteria that can help to identify when processing operations are subject to the requirement for a DPIA. The Working Party 29 Guidelines WP248 state that in most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out, however, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

(5) The lists produced by the competent supervisory authorities support the same objective to identify processing operations likely to result in a high risk and processing operations, which therefore require a DPIA. As such, the criteria developed in the Working Party 29 Guidelines should be applied when assessing whether the draft lists of the competent supervisory authorities does not affect the consistent application of the GDPR.

(6) Twenty-two competent supervisory authorities have submitted their draft lists to the EDPB. A global assessment of these draft lists supports the objective of a consistent application of the GDPR even though the complexity of the subject matter increases.

(7) The opinion of the EDPB shall be adopted pursuant to Article 64 (3) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

I. Summary of the Facts

The Garante per la protezione dei dati personali (hereafter Italian Supervisory Authority) has submitted its draft list to the EDPB. The decision on the completeness of the file was taken on the 11th of July 2018. This period until which the opinion to be adopted has been extended until the 25th of September taking into account the complexity of the subject matter considering that at the same time twenty-two competent supervisory authorities submitted the draft lists and thus the need for a global assessment arose.

¹ WP29, Guidelines on Data Protection Impact Assessment and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP 248 rev. 01).

² EDPB, Endorsement 1/2018.

2. Assessment

2.1 General reasoning of the EDPB regarding the submitted list

Any list submitted to the EDPB has been interpreted as further specifying Art 35.1, which will prevail in any case. Thus, no list can be exhaustive. As the list provided by Italian Supervisory Authority does not explicitly state this, the Board requests this explanation to be added to the document containing the list.

In compliance with article 35.10 GDPR, the Board is of the opinion that if a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of the legal basis the obligation to carry out a DPIA in accordance with paragraphs 1 to 7 of article 35 GDPR does not apply, unless the Member State deems it necessary.

Further, if the Board requests a DPIA for a certain category of processing and an equivalent measure is already required by national law, the Italian Supervisory Authority shall add a reference to this measure.

This opinion does not reflect upon items submitted by the Italian Supervisory Authority, which were deemed outside the scope of Article 35.6 GDPR. This refers to items that neither relate "to the offering of goods or services to data subjects" in several Member States nor to the monitoring of the behaviour of data subjects in several Member States. Additionally, they are not likely to "substantially affect the free movement of personal data within the Union". This is especially the case for items relating to national legislation and in particular where the obligation to carry out a DPIA is stipulated in national legislation. Further, any processing operations that relate to law enforcement were deemed out of scope, as they are not in scope of the GDPR.

The Board has noted that several supervisory authorities have included in their lists some types of processing which are necessarily local processing. Given that only cross border processing and processing that may affect the free flow of personal data and data subjects are concerned by Article 35.6, the Board will not comment on those local processing.

The opinion aims at defining a consistent core of processing operations that are recurrent in the lists provided by the SAs.

This means that, for a limited number of types of processing operations, that will be defined in a harmonised way, all the Supervisory Authorities will require a DPIA to be carried out and the Board will recommend the SAs to amend their lists accordingly in order to ensure consistency.

When this opinion remains silent on DPIA list entries submitted, it means that the Board is not asking the Italian Supervisory Authority to take further action.

Finally, the Board recalls that transparency is key for data controllers and data processors. In order to clarify the entries in the list, the Board is of the opinion that making an explicit

reference in the lists, for each type of processing, to the criteria set out in the guidelines could improve this transparency. Therefore, the Board considers that an explanation on which criteria have been taken into account by the Italian Supervisory Authority to create its list could be added.

2.2 Application of the consistency mechanism to the draft list

The submitted draft list by the Italian Supervisory Authority relates to the offering of goods or services to data subjects, relates to the monitoring of their behaviour in several Member States and/or may substantially affect the free movement of personal data within the Union mainly because the processing operations in the submitted draft list are not limited to data subjects in this country.

2.3 Analysis of the draft list

Taking into account that:

- a. Article 35 (1) GDPR requires a DPIA when the processing activity is likely to result in a high risk to the rights and freedoms of natural persons; and
- b. Article 35 (3) GDPR provides a non-exhaustive list of types of processing that require a DPIA,

the Board is of the opinion that:

INDICATIVE NATURE OF THE LIST

As the list provided by Italian Supervisory Authority does not explicitly state that its list is not exhaustive, the Board requests this explanation to be added to the document containing the list.

REFERENCE TO THE GUIDELINES

The board is of the opinion that the analysis done in the Working Party 29 Guidelines WP248 are a core element for ensuring consistency across the Union. Thus, it requests the different Supervisor Authorities to add a statement to the document containing their list that clarifies that their list is based on these guidelines and that it complements and further specifies the guidelines.

As the document of the Italian Supervisory Authority does not contain such a statement, the Board recommends the Italian Supervisory Authority to amend its document accordingly.

BIOMETRIC DATA

The list submitted by the Italian Supervisory Authority for an opinion of the Board states, that the processing of biometric data falls under the obligation to perform a DPIA on its own. The Board is of the opinion that the processing of biometric data on its own is not necessarily likely to represent a high risk. However, the processing of biometric data for the purpose of uniquely identifying a natural person in conjunction with at least one other criterion requires a DPIA to be carried out. As such, the Board requests the Italian Supervisory Authority to amend its list accordingly, by adding that the item referencing the processing of biometric data for the purpose of uniquely identifying a natural person requires a DPIA to be carried out

only when it is done in conjunction of at least one other criterion, to be applied without prejudice to article 35(3) GDPR.

GENETIC DATA

The list submitted by the Italian Supervisory Authority for an opinion of the Board states, that the processing of genetic data falls under the obligation to perform a DPIA on its own. The Board is of the opinion that the processing of genetic data on its own is not necessarily likely to represent a high risk. However, the processing of genetic data in conjunction with at least one other criterion requires a DPIA to be carried out. As such, the Board requests the Italian Supervisory Authority to amend its list accordingly, by adding that the item referencing the processing of genetic data requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion, to be applied without prejudice to article 35(3) GDPR.

FURTHER PROCESSING

The Board is of the opinion that further processing of personal data should not be a criterion leading to an obligation to do a DPIA, alone or with another criterion. The list submitted by the Italian Supervisory Authority for an opinion of the Board does currently require a DPIA to be carried out for the further processing of personal data. The Board requests the Italian Supervisory Authority to amend its list accordingly, by removing this criterion.

EMPLOYEE MONITORING

The Board is of the opinion that, due to its specific nature, the employee monitoring processing, meeting the criterion of vulnerable data subjects and of systematic monitoring in the guidelines, – could require a DPIA. Given that the list submitted by the Italian Supervisory Authority for an opinion of the Board already envisages this type of processing as requiring a data protection impact assessment, the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248. In addition, the Board is of the opinion that the WP249 of the Article 29 working party remains valid when defining the concept of the systematic processing of employee data.

REFERENCING A SPECIFIC LEGAL BASIS

The Board is of the opinion that the use of a specific legal basis should not be a criterion leading to an obligation to do a DPIA, alone or with another criterion. Given that the list submitted by the Italian Supervisory Authority for an opinion of the Board envisages this type of processing as requiring a data protection impact assessment, the Board requests the Italian Supervisory Authority to amend its list accordingly, by removing the reference to any specific legal basis from its list.

PROCESSING USING NEW/INNOVATIVE TECHNOLOGY

The list submitted by the Italian Supervisory Authority for an opinion of the Board envisages that the use of new or innovative technology, on its own, requires a DPIA. The Board is of the opinion that the use of innovative technology on its own is not necessarily likely to represent a high risk. However, the use of innovative technology in conjunction with at least one other criterion requires a DPIA to be carried out. Therefore, the Board requests the Italian

Supervisory Authority to amend its list accordingly, firstly by referring in their list to innovative technology and secondly by adding that the item requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.

3. Conclusions / Recommendations

The draft list of the Italian Supervisory Authority may lead to an inconsistent application of the requirement for a DPIA and the following changes need to made:

- Regarding the indicative nature of the list: the Board requests an explanation to be added to the document containing the list, stating its non-exhaustive nature.
- Regarding the reference to the guidelines: the Board requests the Italian Supervisory Authority to amend its document accordingly.
- Regarding biometric data: the Board requests the Italian Supervisory Authority to amend its list by adding that the item referencing the processing of biometric data for the purpose of uniquely identifying a natural person requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion
- Regarding genetic data: the Board requests the Italian Supervisory Authority to amend its list by adding that the item referencing the processing of genetic data requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.
- Regarding further processing: the Board requests the Italian Supervisory Authority to amend its list accordingly, by removing this criterion.
- Regarding employment monitoring: the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248.
- Regarding the reference to a specific legal basis: the Board requests the Italian Supervisory Authority to amend its list by removing the reference to any specific legal basis from its list.
- Regarding the processing using new or innovative technology: the Board requests the Italian Supervisory Authority to amend its list firstly by referring in their list to innovative technology and secondly by adding that the item requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.

4. Final Remarks

This opinion is addressed to the Garante per la protezione dei dati personali (Italian Supervisory Authority) and will be made public pursuant to Article 64 (5b) GDPR.

According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 13/2018

on the draft list of the competent supervisory authority of Lithuania

regarding

**the processing operations subject to the requirement of a data protection
impact assessment (Article 35.4 GDPR)**

Adopted on 25th September 2018

Contents

1.	Summary of the Facts	4
2.	Assessment	5
2.1	General reasoning of the EDPB regarding the submitted list	5
2.2	Application of the consistency mechanism to the draft list	6
2.3	Analysis of the draft list.....	6
	Indicative nature of the list.....	6
	Reference to the Guidelines	6
	Biometric data.....	6
	Genetic data.....	7
	Processing for scientific or historical purposes without consent	7
	Exceptions to information to be provided to the data subject according to article 14.5 GDPR	7
	Employee Monitoring	7
	Processing using new/innovative technology	8
3.	Conclusions / Recommendations	8
4.	Final Remarks	9

The European Data Protection Board

Having regard to Article 63, Article 64 (1a), (3) - (8) and Article 35 (1), (3), (4), (6) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (here after GDPR) throughout the European Economic Area. In compliance with article 64.1 GDPR, the Board has to issue an opinion where a supervisory authority intends to adopt a list of processing operations subject to the requirement for a data protection impact assessment pursuant to article 35.4 GDPR. The aim of this opinion is therefore to create a harmonized approach with regard to processing that is cross border or that can affect the free flow of personal data or natural person across the European Union. Even though the GDPR doesn't impose a single list, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by requesting SAs to include some types of processing in their lists, secondly by requesting them to remove some criteria which the Board doesn't consider as necessarily creating high risks for data subjects, and finally by requesting them to use some criteria in a harmonized manner.

(2) With reference to Article 35 (4) and (6) GDPR, the competent supervisory authorities shall establish lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment (hereinafter "DPIA"). They shall, however, apply the consistency mechanism where such lists involve processing operations, which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

(3) While the draft lists of the competent supervisory authorities are subject to the consistency mechanism, this does not mean that the lists should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB assessment/opinion is not to reach a single EU list but rather to avoid significant inconsistencies that may affect the equivalent protection of the data subjects.

(4) The carrying out of a DPIA is only mandatory for the controller pursuant to Article 35 (1) GDPR where processing is "likely to result in a high risk to the rights and freedoms of natural

persons". Article 35 (3) GDPR illustrates what is likely to result in a high risk. This is a non-exhaustive list. The Working Party 29 in the Guidelines on data protection impact assessment¹, as endorsed by the EDPB², has clarified criteria that can help to identify when processing operations are subject to the requirement for a DPIA. The Working Party 29 Guidelines WP248 state that in most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out, however, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

(5) The lists produced by the competent supervisory authorities support the same objective to identify processing operations likely to result in a high risk and processing operations, which therefore require a DPIA. As such, the criteria developed in the Working Party 29 Guidelines should be applied when assessing whether the draft lists of the competent supervisory authorities does not affect the consistent application of the GDPR.

(6) Twenty-two competent supervisory authorities have submitted their draft lists to the EDPB. A global assessment of these draft lists supports the objective of a consistent application of the GDPR even though the complexity of the subject matter increases.

(7) The opinion of the EDPB shall be adopted pursuant to Article 64 (3) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

I. Summary of the Facts

The Valstybinė duomenų apsaugos inspekcija (hereafter Lithuanian Supervisory Authority) has submitted its draft list to the EDPB. The decision on the completeness of the file was taken on the 29th of June 2018. This period until which the opinion to be adopted has been extended until the 25th of September taking into account the complexity of the subject matter considering that at the same time twenty-two competent supervisory authorities submitted the draft lists and thus the need for a global assessment arose.

¹ WP29, Guidelines on Data Protection Impact Assessment and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP 248 rev. 01).

² EDPB, Endorsement 1/2018.

2. Assessment

2.1 General reasoning of the EDPB regarding the submitted list

Any list submitted to the EDPB has been interpreted as further specifying Art 35.1, which will prevail in any case. Thus, no list can be exhaustive. As the list provided by Lithuanian Supervisory Authority does not explicitly state this, the Board requests this explanation to be added to the document containing the list.

In compliance with article 35.10 GDPR, the Board is of the opinion that if a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of the legal basis the obligation to carry out a DPIA in accordance with paragraphs 1 to 7 of article 35 GDPR does not apply, unless the Member State deems it necessary.

Further, if the Board requests a DPIA for a certain category of processing and an equivalent measure is already required by national law, the Lithuanian Supervisory Authority shall add a reference to this measure.

This opinion does not reflect upon items submitted by the Lithuanian Supervisory Authority, which were deemed outside the scope of Article 35.6 GDPR. This refers to items that neither relate “to the offering of goods or services to data subjects” in several Member States nor to the monitoring of the behaviour of data subjects in several Member States. Additionally, they are not likely to “substantially affect the free movement of personal data within the Union”. This is especially the case for items relating to national legislation and in particular where the obligation to carry out a DPIA is stipulated in national legislation. Further, any processing operations that relate to law enforcement were deemed out of scope, as they are not in scope of the GDPR.

The Board has noted that several supervisory authorities have included in their lists some types of processing which are necessarily local processing. Given that only cross border processing and processing that may affect the free flow of personal data and data subjects are concerned by Article 35.6, the Board will not comment on those local processing.

The opinion aims at defining a consistent core of processing operations that are recurrent in the lists provided by the SAs.

This means that, for a limited number of types of processing operations, that will be defined in a harmonised way, all the Supervisory Authorities will require a DPIA to be carried out and the Board will recommend the SAs to amend their lists accordingly in order to ensure consistency.

When this opinion remains silent on DPIA list entries submitted, it means that the Board is not asking the Lithuanian Supervisory Authority to take further action.

Finally, the Board recalls that transparency is key for data controllers and data processors. In order to clarify the entries in the list, the Board is of the opinion that making an explicit

reference in the lists, for each type of processing, to the criteria set out in the guidelines could improve this transparency. Therefore, the Board considers that an explanation on which criteria have been taken into account by the Lithuanian Supervisory Authority to create its list could be added.

2.2 Application of the consistency mechanism to the draft list

The submitted draft list by the Lithuanian Supervisory Authority relates to the offering of goods or services to data subjects, relates to the monitoring of their behaviour in several Member States and/or may substantially affect the free movement of personal data within the Union mainly because the processing operations in the submitted draft list are not limited to data subjects in this country.

2.3 Analysis of the draft list

Taking into account that:

- a. Article 35 (1) GDPR requires a DPIA when the processing activity is likely to result in a high risk to the rights and freedoms of natural persons; and
- b. Article 35 (3) GDPR provides a non-exhaustive list of types of processing that require a DPIA,

the Board is of the opinion that:

INDICATIVE NATURE OF THE LIST

As the list provided by Lithuanian Supervisory Authority does not explicitly state that its list is not exhaustive, the Board requests this explanation to be added to the document containing the list.

REFERENCE TO THE GUIDELINES

The board is of the opinion that the analysis done in the Working Party 29 Guidelines WP248 are a core element for ensuring consistency across the Union. Thus, it requests the different Supervisor Authorities to add a statement to the document containing their list that clarifies that their list is based on these guidelines and that it complements and further specifies the guidelines.

As the document of the Lithuanian Supervisory Authority does not contain such a statement, the Board recommends the Lithuanian Supervisory Authority to amend its document accordingly.

BIOMETRIC DATA

The list submitted by the Lithuanian Supervisory Authority for an opinion of the Board states, that the processing of biometric data falls under the obligation to perform a DPIA on its own. The Board is of the opinion that the processing of biometric data on its own is not necessarily likely to represent a high risk. However, the processing of biometric data for the purpose of uniquely identifying a natural person in conjunction with at least one other criterion requires a DPIA to be carried out. As such, the Board requests the Lithuanian Supervisory Authority to amend its list accordingly, by adding that the item referencing the processing of biometric

data for the purpose of uniquely identifying a natural person requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion, to be applied without prejudice to article 35(3) GDPR.

GENETIC DATA

The list submitted by the Lithuanian Supervisory Authority for an opinion of the Board states, that the processing of genetic data falls under the obligation to perform a DPIA on its own. The Board is of the opinion that the processing of genetic data on its own is not necessarily likely to represent a high risk. However, the processing of genetic data in conjunction with at least one other criterion requires a DPIA to be carried out. As such, the Board requests the Lithuanian Supervisory Authority to amend its list accordingly, by adding that the item referencing the processing of genetic data requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion, to be applied without prejudice to article 35(3) GDPR.

PROCESSING FOR SCIENTIFIC OR HISTORICAL PURPOSES WITHOUT CONSENT

The Board is of the opinion that the processing of personal data for scientific or historical purposes on its own is not necessarily likely to represent a high risk. However, the processing of personal data for scientific or historical purpose in conjunction with at least one other criterion does require a DPIA to be carried out. The list submitted by the Lithuanian Supervisory Authority for an opinion of the Board does currently require a DPIA to be carried out when there is a processing of personal data for scientific or historical purpose on its own. The Board requests the Lithuanian Supervisory Authority to amend its list accordingly, by adding that the item referencing the processing of personal data for scientific or historical purpose requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.

EXCEPTIONS TO INFORMATION TO BE PROVIDED TO THE DATA SUBJECT ACCORDING TO ARTICLE 14.5 GDPR

The Board is of the opinion that types of processing activities that could deprive the data subjects from their rights do not represent a high risk on their own. Therefore, a processing activity conducted by the controller under article 14 GDPR and where the information to be given to the data subjects is subject to an exemption under article 14.5 (b)-(d) could require a DPIA to be carried out only in conjunction with at least one other criterion. The list submitted by the Lithuanian Supervisory Authority for an opinion of the Board does currently require a DPIA to be done for the processing of data where article 14(5), para (b), (c) and (d) applies on its own. The Board requests the Lithuanian Supervisory Authority to amend its list accordingly, by adapting the list entry by adding that it requires a DPIA only in conjunction with at least one other criterion.

EMPLOYEE MONITORING

The Board is of the opinion that, due to its specific nature, the employee monitoring processing, meeting the criterion of vulnerable data subjects and of systematic monitoring in the guidelines, – could require a DPIA. Given that the list submitted by the Lithuanian

Supervisory Authority for an opinion of the Board already envisages this type of processing as requiring a data protection impact assessment, the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248. In addition, the Board is of the opinion that the WP249 of the Article 29 working party remains valid when defining the concept of the systematic processing of employee data.

PROCESSING USING NEW/INNOVATIVE TECHNOLOGY

The list submitted by the Lithuanian Supervisory Authority for an opinion of the Board envisages that the use of new or innovative technology, on its own, requires a DPIA. The Board is of the opinion that the use of innovative technology on its own is not necessarily likely to represent a high risk. However, the use of innovative technology in conjunction with at least one other criterion requires a DPIA to be carried out. Therefore, the Board requests the Lithuanian Supervisory Authority to amend its list accordingly, firstly by referring in their list to innovative technology and secondly by adding that the item requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.

3. Conclusions / Recommendations

The draft list of the Lithuanian Supervisory Authority may lead to an inconsistent application of the requirement for a DPIA and the following changes need to made:

- Regarding the indicative nature of the list: the Board requests an explanation to be added to the document containing the list, stating its non-exhaustive nature.
- Regarding the reference to the guidelines: the Board requests the Lithuanian Supervisory Authority to amend its document accordingly.
- Regarding biometric data: the Board requests the Lithuanian Supervisory Authority to amend its list by adding that the item referencing the processing of biometric data for the purpose of uniquely identifying a natural person requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion
- Regarding genetic data: the Board requests the Lithuanian Supervisory Authority to amend its list by adding that the item referencing the processing of genetic data requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.
- Regarding processing of personal data for scientific or historical purposes: the Board requests the Lithuanian Supervisory Authority to amend its list by adding that the item referencing the processing of personal data for scientific or historical purpose requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.
- Regarding the exceptions to the information to be given to the data subjects according to article 14.5 GDPR: the Board requests the Lithuanian Supervisory Authority to amend its list by adding that it requires a DPIA only in conjunction with at least one other criterion.

- Regarding employment monitoring: the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248.
- Regarding processing using new or innovative technology: the Board requests the Lithuanian Supervisory Authority to amend its list firstly by referring in their list to innovative technology and secondly by adding that the item requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.

4. Final Remarks

This opinion is addressed to the Valstybinė duomenų apsaugos inspekcija (Lithuanian Supervisory Authority) and will be made public pursuant to Article 64 (5b) GDPR.

According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 14/2018

on the draft list of the competent supervisory authority of Latvia

regarding

**the processing operations subject to the requirement of a data protection
impact assessment (Article 35.4 GDPR)**

Adopted on 25th September 2018

Contents

1.	Summary of the Facts	4
2.	Assessment	5
2.1	General reasoning of the EDPB regarding the submitted list	5
2.2	Application of the consistency mechanism to the draft list	6
2.3	Analysis of the draft list.....	6
	Indicative nature of the list.....	6
	Reference to the Guidelines	6
	Biometric data.....	6
	Genetic data.....	7
	Location data	7
	Data collected via third parties (article 19 GDPR)	7
	Processing for scientific or historical purposes without consent	7
	Employee Monitoring	7
	International transfers	8
	Processing posing a significant risk.....	8
	Processing using new/innovative technology	8
3.	Conclusions / Recommendations	8
4.	Final Remarks	9

The European Data Protection Board

Having regard to Article 63, Article 64 (1a), (3) - (8) and Article 35 (1), (3), (4), (6) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (here after GDPR) throughout the European Economic Area. In compliance with article 64.1 GDPR, the Board has to issue an opinion where a supervisory authority intends to adopt a list of processing operations subject to the requirement for a data protection impact assessment pursuant to article 35.4 GDPR. The aim of this opinion is therefore to create a harmonized approach with regard to processing that is cross border or that can affect the free flow of personal data or natural person across the European Union. Even though the GDPR doesn't impose a single list, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by requesting SAs to include some types of processing in their lists, secondly by requesting them to remove some criteria which the Board doesn't consider as necessarily creating high risks for data subjects, and finally by requesting them to use some criteria in a harmonized manner.

(2) With reference to Article 35 (4) and (6) GDPR, the competent supervisory authorities shall establish lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment (hereinafter "DPIA"). They shall, however, apply the consistency mechanism where such lists involve processing operations, which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

(3) While the draft lists of the competent supervisory authorities are subject to the consistency mechanism, this does not mean that the lists should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB assessment/opinion is not to reach a single EU list but rather to avoid significant inconsistencies that may affect the equivalent protection of the data subjects.

(4) The carrying out of a DPIA is only mandatory for the controller pursuant to Article 35 (1) GDPR where processing is "likely to result in a high risk to the rights and freedoms of natural

persons". Article 35 (3) GDPR illustrates what is likely to result in a high risk. This is a non-exhaustive list. The Working Party 29 in the Guidelines on data protection impact assessment¹, as endorsed by the EDPB², has clarified criteria that can help to identify when processing operations are subject to the requirement for a DPIA. The Working Party 29 Guidelines WP248 state that in most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out, however, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

(5) The lists produced by the competent supervisory authorities support the same objective to identify processing operations likely to result in a high risk and processing operations, which therefore require a DPIA. As such, the criteria developed in the Working Party 29 Guidelines should be applied when assessing whether the draft lists of the competent supervisory authorities does not affect the consistent application of the GDPR.

(6) Twenty-two competent supervisory authorities have submitted their draft lists to the EDPB. A global assessment of these draft lists supports the objective of a consistent application of the GDPR even though the complexity of the subject matter increases.

(7) The opinion of the EDPB shall be adopted pursuant to Article 64 (3) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

I. Summary of the Facts

The Datu valsts inpekcija (hereafter Latvian Supervisory Authority) has submitted its draft list to the EDPB. The decision on the completeness of the file was taken on the 10th of July 2018. This period until which the opinion to be adopted has been extended until the 25th of September taking into account the complexity of the subject matter considering that at the same time twenty-two competent supervisory authorities submitted the draft lists and thus the need for a global assessment arose.

¹ WP29, Guidelines on Data Protection Impact Assessment and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP 248 rev. 01).

² EDPB, Endorsement 1/2018.

2. Assessment

2.1 General reasoning of the EDPB regarding the submitted list

Any list submitted to the EDPB has been interpreted as further specifying Art 35.1, which will prevail in any case. Thus, no list can be exhaustive. As the list provided by Latvian Supervisory Authority does not explicitly state this, the Board requests this explanation to be added to the document containing the list.

In compliance with article 35.10 GDPR, the Board is of the opinion that if a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of the legal basis the obligation to carry out a DPIA in accordance with paragraphs 1 to 7 of article 35 GDPR does not apply, unless the Member State deems it necessary.

Further, if the Board requests a DPIA for a certain category of processing and an equivalent measure is already required by national law, the Latvian Supervisory Authority shall add a reference to this measure.

This opinion does not reflect upon items submitted by the Latvian Supervisory Authority, which were deemed outside the scope of Article 35.6 GDPR. This refers to items that neither relate “to the offering of goods or services to data subjects” in several Member States nor to the monitoring of the behaviour of data subjects in several Member States. Additionally, they are not likely to “substantially affect the free movement of personal data within the Union”. This is especially the case for items relating to national legislation and in particular where the obligation to carry out a DPIA is stipulated in national legislation. Further, any processing operations that relate to law enforcement were deemed out of scope, as they are not in scope of the GDPR.

The Board has noted that several supervisory authorities have included in their lists some types of processing which are necessarily local processing. Given that only cross border processing and processing that may affect the free flow of personal data and data subjects are concerned by Article 35.6, the Board will not comment on those local processing.

The opinion aims at defining a consistent core of processing operations that are recurrent in the lists provided by the SAs.

This means that, for a limited number of types of processing operations, that will be defined in a harmonised way, all the Supervisory Authorities will require a DPIA to be carried out and the Board will recommend the SAs to amend their lists accordingly in order to ensure consistency.

When this opinion remains silent on DPIA list entries submitted, it means that the Board is not asking the Latvian Supervisory Authority to take further action.

Finally, the Board recalls that transparency is key for data controllers and data processors. In order to clarify the entries in the list, the Board is of the opinion that making an explicit

reference in the lists, for each type of processing, to the criteria set out in the guidelines could improve this transparency. Therefore, the Board considers that an explanation on which criteria have been taken into account by the Latvian Supervisory Authority to create its list could be added.

2.2 Application of the consistency mechanism to the draft list

The submitted draft list by the Latvian Supervisory Authority relates to the offering of goods or services to data subjects, relates to the monitoring of their behaviour in several Member States and/or may substantially affect the free movement of personal data within the Union mainly because the processing operations in the submitted draft list are not limited to data subjects in this country.

2.3 Analysis of the draft list

Taking into account that:

- a. Article 35 (1) GDPR requires a DPIA when the processing activity is likely to result in a high risk to the rights and freedoms of natural persons; and
- b. Article 35 (3) GDPR provides a non-exhaustive list of types of processing that require a DPIA,

the Board is of the opinion that:

INDICATIVE NATURE OF THE LIST

As the list provided by Latvian Supervisory Authority does not explicitly state that its list is not exhaustive, the Board requests this explanation to be added to the document containing the list.

REFERENCE TO THE GUIDELINES

The board is of the opinion that the analysis done in the Working Party 29 Guidelines WP248 are a core element for ensuring consistency across the Union. Thus, it requests the different Supervisor Authorities to add a statement to the document containing their list that clarifies that their list is based on these guidelines and that it complements and further specifies the guidelines.

As the document of the Latvian Supervisory Authority does not contain such a statement, the Board recommends the Latvian Supervisory Authority to amend its document accordingly.

BIOMETRIC DATA

The list submitted by the Latvian Supervisory Authority for an opinion of the Board does not currently require a DPIA to be done for the processing of biometric data for the purpose of uniquely identifying a natural person. As such, the Board requests the Latvian Supervisory Authority to amend its list accordingly, by adding explicitly the processing of biometric data for the purpose of uniquely identifying a natural person in conjunction with at least one other criterion to its list, to be applied without prejudice to article 35(3) GDPR.

GENETIC DATA

The list submitted by the Latvian Supervisory Authority for an opinion of the Board states, that the processing of genetic data falls under the obligation to perform a DPIA on its own. The Board is of the opinion that the processing of genetic data on its own is not necessarily likely to represent a high risk. However, the processing of genetic data in conjunction with at least one other criterion requires a DPIA to be carried out. As such, the Board requests the Latvian Supervisory Authority to amend its list accordingly, by adding that the item referencing the processing of genetic data requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion, to be applied without prejudice to article 35(3) GDPR.

LOCATION DATA

The Board is of the opinion that consistency is one of the basic principle of the GDPR. The Board notes that a majority of the lists submitted explicitly contain a reference to the processing of location data. As the list submitted by the Latvian Supervisory Authority for an opinion do not contain such a reference, the Board encourages the Latvian Supervisory Authority to include the processing of location data in its list, together with another criterion.

DATA COLLECTED VIA THIRD PARTIES (ARTICLE 19 GDPR)

The Board is of the opinion that types of processing activities that could deprive the data subjects from their rights in conjunction with at least one other criterion represent a high risk. Further, the Board is of the opinion that a processing activity conducted by the controller under article 19 GDPR and where the information of recipients would prove impossible or require a disproportionate effort only requires a DPIA to be carried out when this processing involves at least one other criterion. The list submitted by the Latvian Supervisory Authority for an opinion of the Board states that this type of processing in conjunction with at least one other criterion falls under the obligation to perform a DPIA. The Board takes note of the inclusion of this criterion in the list.

PROCESSING FOR SCIENTIFIC OR HISTORICAL PURPOSES WITHOUT CONSENT

The Board is of the opinion that the processing of personal data for scientific or historical purposes on its own is not necessarily likely to represent a high risk. However, the processing of personal data for scientific or historical purpose in conjunction with at least one other criterion does require a DPIA to be carried out. The list submitted by the Latvian Supervisory Authority for an opinion of the Board does currently require a DPIA to be carried out when there is a processing of personal data for scientific or historical purpose on its own. The Board requests the Latvian Supervisory Authority to amend its list accordingly, by adding that the item referencing the processing of personal data for scientific or historical purpose requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.

EMPLOYEE MONITORING

The Board is of the opinion that, due to its specific nature, the employee monitoring processing, meeting the criterion of vulnerable data subjects and of systematic monitoring in the guidelines, – could require a DPIA. Given that the list submitted by the Latvian Supervisory

Authority for an opinion of the Board already envisages this type of processing as requiring a data protection impact assessment, the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248. In addition, the Board is of the opinion that the WP249 of the Article 29 working party remains valid when defining the concept of the systematic processing of employee data.

INTERNATIONAL TRANSFERS

The Board is of the opinion that the processing made in the context of international transfers should not be a criterion leading to an obligation to do a DPIA, alone or with another criterion. Given that the list submitted by the Latvian Supervisory Authority for an opinion of the Board envisages this type of processing as requiring a data protection impact assessment, the Board requests the Latvian Supervisory Authority to amend its list accordingly, by removing the reference to international transfers from its list.

PROCESSING POSING A SIGNIFICANT RISK

The Board is of the opinion that the term “significant risk”, as used under item 6 of the list of processing operations requiring a DPIA submitted by the Latvian Supervisory Authority, is equivalent to the term “likely to result in a high risk” as stated by article 35.1 GDPR. Therefore, the Board requests the Latvian Supervisory Authority to amend its list accordingly, by removing item 6 from its list.

PROCESSING USING NEW/INNOVATIVE TECHNOLOGY

The list submitted by the Latvian Supervisory Authority for an opinion of the Board envisages that the use of new or innovative technology, on its own, requires a DPIA. The Board is of the opinion that the use of innovative technology on its own is not necessarily likely to represent a high risk. However, the use of innovative technology in conjunction with at least one other criterion requires a DPIA to be carried out. Therefore, the Board requests the Latvian Supervisory Authority to amend its list accordingly, firstly by referring in their list to innovative technology and secondly by adding that the item requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.

3. Conclusions / Recommendations

The draft list of the Latvian Supervisory Authority may lead to an inconsistent application of the requirement for a DPIA and the following changes need to be made:

- Regarding the indicative nature of the list: the Board requests an explanation to be added to the document containing the list, stating its non-exhaustive nature.
- Regarding the reference to the guidelines: the Board requests the Latvian Supervisory Authority to amend its document accordingly.
- Regarding biometric data: the Board requests the Latvian Supervisory Authority to amend its list accordingly, by adding explicitly the processing of biometric data for the purpose of uniquely identifying a natural person in conjunction with at least one other criterion to its list.

- Regarding genetic data: the Board requests the Latvian Supervisory Authority to amend its list by adding that the item referencing the processing of genetic data requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.
- Regarding location data: the Board encourages the Latvian Supervisory Authority to include the processing of location data in its list, together with another criterion.
- Regarding processing of personal data for scientific or historical purposes: the Board requests the Latvian Supervisory Authority to amend its list by adding that the item referencing the processing of personal data for scientific or historical purpose requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.
- Regarding employment monitoring: the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248.
- Regarding international transfers: the Board requests the Latvian Supervisory Authority to amend its list by removing the reference to international transfers in its list.
- Regarding processing posing a significant risk: the Board requests the Latvian Supervisory Authority to amend its list by removing item 6 from its list.
- Regarding processing using new or innovative technology: the Board requests the Latvian Supervisory Authority to amend its list firstly by referring in their list to innovative technology and secondly by adding that the item requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.

4. Final Remarks

This opinion is addressed to the Datu valsts inpekcija (Latvian Supervisory Authority) and will be made public pursuant to Article 64 (5b) GDPR.

According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 15/2018

on the draft list of the competent supervisory authority of Malta

regarding

**the processing operations subject to the requirement of a data protection
impact assessment (Article 35.4 GDPR)**

Adopted on 25th September 2018

Contents

1.	Summary of the Facts	4
2.	Assessment	5
2.1	General reasoning of the EDPB regarding the submitted list	5
2.2	Application of the consistency mechanism to the draft list	6
2.3	Analysis of the draft list.....	6
	Indicative nature of the list.....	6
	Reference to the Guidelines	6
	Biometric data.....	6
	Genetic data.....	7
	Further processing	7
	Employee Monitoring	7
	Processing using new/innovative technology	7
3.	Conclusions / Recommendations	8
4.	Final Remarks	8

The European Data Protection Board

Having regard to Article 63, Article 64 (1a), (3) - (8) and Article 35 (1), (3), (4), (6) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (here after GDPR) throughout the European Economic Area. In compliance with article 64.1 GDPR, the Board has to issue an opinion where a supervisory authority intends to adopt a list of processing operations subject to the requirement for a data protection impact assessment pursuant to article 35.4 GDPR. The aim of this opinion is therefore to create a harmonized approach with regard to processing that is cross border or that can affect the free flow of personal data or natural person across the European Union. Even though the GDPR doesn't impose a single list, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by requesting SAs to include some types of processing in their lists, secondly by requesting them to remove some criteria which the Board doesn't consider as necessarily creating high risks for data subjects, and finally by requesting them to use some criteria in a harmonized manner.

(2) With reference to Article 35 (4) and (6) GDPR, the competent supervisory authorities shall establish lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment (hereinafter "DPIA"). They shall, however, apply the consistency mechanism where such lists involve processing operations, which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

(3) While the draft lists of the competent supervisory authorities are subject to the consistency mechanism, this does not mean that the lists should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB assessment/opinion is not to reach a single EU list but rather to avoid significant inconsistencies that may affect the equivalent protection of the data subjects.

(4) The carrying out of a DPIA is only mandatory for the controller pursuant to Article 35 (1) GDPR where processing is "likely to result in a high risk to the rights and freedoms of natural

persons". Article 35 (3) GDPR illustrates what is likely to result in a high risk. This is a non-exhaustive list. The Working Party 29 in the Guidelines on data protection impact assessment¹, as endorsed by the EDPB², has clarified criteria that can help to identify when processing operations are subject to the requirement for a DPIA. The Working Party 29 Guidelines WP248 state that in most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out, however, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

(5) The lists produced by the competent supervisory authorities support the same objective to identify processing operations likely to result in a high risk and processing operations, which therefore require a DPIA. As such, the criteria developed in the Working Party 29 Guidelines should be applied when assessing whether the draft lists of the competent supervisory authorities does not affect the consistent application of the GDPR.

(6) Twenty-two competent supervisory authorities have submitted their draft lists to the EDPB. A global assessment of these draft lists supports the objective of a consistent application of the GDPR even though the complexity of the subject matter increases.

(7) The opinion of the EDPB shall be adopted pursuant to Article 64 (3) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

I. Summary of the Facts

The Office of the Information and Data Protection Commissioner (hereafter Maltese Supervisory Authority) has submitted its draft list to the EDPB. The decision on the completeness of the file was taken on the 10th of July 2018. This period until which the opinion to be adopted has been extended until the 25th of September taking into account the complexity of the subject matter considering that at the same time twenty-two competent supervisory authorities submitted the draft lists and thus the need for a global assessment arose.

¹ WP29, Guidelines on Data Protection Impact Assessment and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP 248 rev. 01).

² EDPB, Endorsement 1/2018.

2. Assessment

2.1 General reasoning of the EDPB regarding the submitted list

Any list submitted to the EDPB has been interpreted as further specifying Art 35.1, which will prevail in any case. Thus, no list can be exhaustive. As the list provided by Maltese Supervisory Authority does not explicitly state this, the Board requests this explanation to be added to the document containing the list.

In compliance with article 35.10 GDPR, the Board is of the opinion that if a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of the legal basis the obligation to carry out a DPIA in accordance with paragraphs 1 to 7 of article 35 GDPR does not apply, unless the Member State deems it necessary.

Further, if the Board requests a DPIA for a certain category of processing and an equivalent measure is already required by national law, the Maltese Supervisory Authority shall add a reference to this measure.

This opinion does not reflect upon items submitted by the Maltese Supervisory Authority, which were deemed outside the scope of Article 35.6 GDPR. This refers to items that neither relate “to the offering of goods or services to data subjects” in several Member States nor to the monitoring of the behaviour of data subjects in several Member States. Additionally, they are not likely to “substantially affect the free movement of personal data within the Union”. This is especially the case for items relating to national legislation and in particular where the obligation to carry out a DPIA is stipulated in national legislation. Further, any processing operations that relate to law enforcement were deemed out of scope, as they are not in scope of the GDPR.

The Board has noted that several supervisory authorities have included in their lists some types of processing which are necessarily local processing. Given that only cross border processing and processing that may affect the free flow of personal data and data subjects are concerned by Article 35.6, the Board will not comment on those local processing.

The opinion aims at defining a consistent core of processing operations that are recurrent in the lists provided by the SAs.

This means that, for a limited number of types of processing operations, that will be defined in a harmonised way, all the Supervisory Authorities will require a DPIA to be carried out and the Board will recommend the SAs to amend their lists accordingly in order to ensure consistency.

When this opinion remains silent on DPIA list entries submitted, it means that the Board is not asking the Maltese Supervisory Authority to take further action.

Finally, the Board recalls that transparency is key for data controllers and data processors. In order to clarify the entries in the list, the Board is of the opinion that making an explicit

reference in the lists, for each type of processing, to the criteria set out in the guidelines could improve this transparency. Therefore, the Board considers that an explanation on which criteria have been taken into account by the Maltese Supervisory Authority to create its list could be added.

2.2 Application of the consistency mechanism to the draft list

The submitted draft list by the Maltese Supervisory Authority relates to the offering of goods or services to data subjects, relates to the monitoring of their behaviour in several Member States and/or may substantially affect the free movement of personal data within the Union mainly because the processing operations in the submitted draft list are not limited to data subjects in this country.

2.3 Analysis of the draft list

Taking into account that:

- a. Article 35 (1) GDPR requires a DPIA when the processing activity is likely to result in a high risk to the rights and freedoms of natural persons; and
- b. Article 35 (3) GDPR provides a non-exhaustive list of types of processing that require a DPIA,

the Board is of the opinion that:

INDICATIVE NATURE OF THE LIST

As the list provided by Maltese Supervisory Authority does not explicitly state that its list is not exhaustive, the Board requests this explanation to be added to the document containing the list.

REFERENCE TO THE GUIDELINES

The board is of the opinion that the analysis done in the Working Party 29 Guidelines WP248 are a core element for ensuring consistency across the Union. Thus, it requests the different Supervisor Authorities to add a statement to the document containing their list that clarifies that their list is based on these guidelines and that it complements and further specifies the guidelines.

As the document of the Maltese Supervisory Authority does not contain such a statement, the Board recommends the Maltese Supervisory Authority to amend its document accordingly.

BIOMETRIC DATA

The list submitted by the Maltese Supervisory Authority for an opinion of the Board states, that the processing of biometric data falls under the obligation to perform a DPIA on its own. The Board is of the opinion that the processing of biometric data on its own is not necessarily likely to represent a high risk. However, the processing of biometric data for the purpose of uniquely identifying a natural person in conjunction with at least one other criterion requires a DPIA to be carried out. As such, the Board requests the Maltese Supervisory Authority to amend its list accordingly, by adding that the item referencing the processing of biometric

data for the purpose of uniquely identifying a natural person requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion, to be applied without prejudice to article 35(3) GDPR.

GENETIC DATA

The list submitted by the Maltese Supervisory Authority for an opinion of the Board states, that the processing of genetic data falls under the obligation to perform a DPIA on its own. The Board is of the opinion that the processing of genetic data on its own is not necessarily likely to represent a high risk. However, the processing of genetic data in conjunction with at least one other criterion requires a DPIA to be carried out. As such, the Board requests the Maltese Supervisory Authority to amend its list accordingly, by adding that the item referencing the processing of genetic data requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion, to be applied without prejudice to article 35(3) GDPR.

FURTHER PROCESSING

The Board is of the opinion that further processing of personal data should not be a criterion leading to an obligation to do a DPIA, alone or with another criterion. The list submitted by the Maltese Supervisory Authority for an opinion of the Board does currently require a DPIA to be carried out for the further processing of personal data. The Board requests the Maltese Supervisory Authority to amend its list accordingly, by removing this criterion.

EMPLOYEE MONITORING

The Board is of the opinion that, due to its specific nature, the employee monitoring processing, meeting the criterion of vulnerable data subjects and of systematic monitoring in the guidelines, – could require a DPIA. Given that the list submitted by the Maltese Supervisory Authority for an opinion of the Board already envisages this type of processing as requiring a data protection impact assessment, the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248. In addition, the Board is of the opinion that the WP249 of the Article 29 working party remains valid when defining the concept of the systematic processing of employee data.

PROCESSING USING NEW/INNOVATIVE TECHNOLOGY

The list submitted by the Maltese Supervisory Authority for an opinion of the Board envisages that the use of new or innovative technology, on its own, requires a DPIA. The Board is of the opinion that the use of innovative technology on its own is not necessarily likely to represent a high risk. However, the use of innovative technology in conjunction with at least one other criterion requires a DPIA to be carried out. Therefore, the Board requests the Maltese Supervisory Authority to amend its list accordingly, firstly by referring in their list to innovative technology and secondly by adding that the item requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.

3. Conclusions / Recommendations

The draft list of the Maltese Supervisory Authority may lead to an inconsistent application of the requirement for a DPIA and the following changes need to made:

- Regarding the indicative nature of the list: the Board requests an explanation to be added to the document containing the list, stating its non-exhaustive nature.
- Regarding the reference to the guidelines: the Board requests the Maltese Supervisory Authority to amend its document accordingly.
- Regarding biometric data: the Board requests the Maltese Supervisory Authority to amend its list by adding that the item referencing the processing of biometric data for the purpose of uniquely identifying a natural person requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion
- Regarding genetic data: the Board requests the Maltese Supervisory Authority to amend its list by adding that the item referencing the processing of genetic data requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.
- Regarding further processing: the Board requests the Maltese Supervisory Authority to amend its list accordingly, by removing this criterion.
- Regarding employment monitoring: the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248.
- Regarding processing using new or innovative technology: the Board requests the Maltese Supervisory Authority to amend its list firstly by referring in their list to innovative technology and secondly by adding that the item requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.

4. Final Remarks

This opinion is addressed to the Office of the Information and Data Protection Commissioner (Maltese Supervisory Authority) and will be made public pursuant to Article 64 (5b) GDPR.

According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 16/2018

**on the draft list of the competent supervisory authority of the Netherlands
regarding
the processing operations subject to the requirement of a data protection
impact assessment (Article 35.4 GDPR)**

Adopted on 25th September 2018

Contents

1.	Summary of the Facts	4
2.	Assessment	5
2.1	General reasoning of the EDPB regarding the submitted list	5
2.2	Application of the consistency mechanism to the draft list	6
2.3	Analysis of the draft list.....	6
	Biometric data.....	6
	Genetic data.....	6
	Location data	6
	Exceptions to information to be provided to the data subject according to article 14.5 GDPR	7
	Employee Monitoring	7
	Processing using new/innovative technology	7
3.	Conclusions / Recommendations	7
4.	Final Remarks.....	8

The European Data Protection Board

Having regard to Article 63, Article 64 (1a), (3) - (8) and Article 35 (1), (3), (4), (6) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (here after GDPR) throughout the European Economic Area. In compliance with article 64.1 GDPR, the Board has to issue an opinion where a supervisory authority intends to adopt a list of processing operations subject to the requirement for a data protection impact assessment pursuant to article 35.4 GDPR. The aim of this opinion is therefore to create a harmonized approach with regard to processing that is cross border or that can affect the free flow of personal data or natural person across the European Union. Even though the GDPR doesn't impose a single list, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by requesting SAs to include some types of processing in their lists, secondly by requesting them to remove some criteria which the Board doesn't consider as necessarily creating high risks for data subjects, and finally by requesting them to use some criteria in a harmonized manner.

(2) With reference to Article 35 (4) and (6) GDPR, the competent supervisory authorities shall establish lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment (hereinafter "DPIA"). They shall, however, apply the consistency mechanism where such lists involve processing operations, which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

(3) While the draft lists of the competent supervisory authorities are subject to the consistency mechanism, this does not mean that the lists should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB assessment/opinion is not to reach a single EU list but rather to avoid significant inconsistencies that may affect the equivalent protection of the data subjects.

(4) The carrying out of a DPIA is only mandatory for the controller pursuant to Article 35 (1) GDPR where processing is "likely to result in a high risk to the rights and freedoms of natural

persons". Article 35 (3) GDPR illustrates what is likely to result in a high risk. This is a non-exhaustive list. The Working Party 29 in the Guidelines on data protection impact assessment¹, as endorsed by the EDPB², has clarified criteria that can help to identify when processing operations are subject to the requirement for a DPIA. The Working Party 29 Guidelines WP248 state that in most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out, however, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

(5) The lists produced by the competent supervisory authorities support the same objective to identify processing operations likely to result in a high risk and processing operations, which therefore require a DPIA. As such, the criteria developed in the Working Party 29 Guidelines should be applied when assessing whether the draft lists of the competent supervisory authorities does not affect the consistent application of the GDPR.

(6) Twenty-two competent supervisory authorities have submitted their draft lists to the EDPB. A global assessment of these draft lists supports the objective of a consistent application of the GDPR even though the complexity of the subject matter increases.

(7) The opinion of the EDPB shall be adopted pursuant to Article 64 (3) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

I. Summary of the Facts

The Autoriteit Persoonsgegevens (hereafter Dutch Supervisory Authority) has submitted its draft list to the EDPB. The decision on the completeness of the file was taken on the 11th of July 2018. This period until which the opinion to be adopted has been extended until the 25th of September taking into account the complexity of the subject matter considering that at the same time twenty-two competent supervisory authorities submitted the draft lists and thus the need for a global assessment arose.

¹ WP29, Guidelines on Data Protection Impact Assessment and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP 248 rev. 01).

² EDPB, Endorsement 1/2018.

2. Assessment

2.1 General reasoning of the EDPB regarding the submitted list

Any list submitted to the EDPB has been interpreted as further specifying Art 35.1, which will prevail in any case. Thus, no list can be exhaustive.

In compliance with article 35.10 GDPR, the Board is of the opinion that if a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of the legal basis the obligation to carry out a DPIA in accordance with paragraphs 1 to 7 of article 35 GDPR does not apply, unless the Member State deems it necessary.

Further, if the Board requests a DPIA for a certain category of processing and an equivalent measure is already required by national law, the Dutch Supervisory Authority shall add a reference to this measure.

This opinion does not reflect upon items submitted by the Dutch Supervisory Authority, which were deemed outside the scope of Article 35.6 GDPR. This refers to items that neither relate "to the offering of goods or services to data subjects" in several Member States nor to the monitoring of the behaviour of data subjects in several Member States. Additionally, they are not likely to "substantially affect the free movement of personal data within the Union". This is especially the case for items relating to national legislation and in particular where the obligation to carry out a DPIA is stipulated in national legislation. Further, any processing operations that relate to law enforcement were deemed out of scope, as they are not in scope of the GDPR.

The Board has noted that several supervisory authorities have included in their lists some types of processing which are necessarily local processing. Given that only cross border processing and processing that may affect the free flow of personal data and data subjects are concerned by Article 35.6, the Board will not comment on those local processing.

The opinion aims at defining a consistent core of processing operations that are recurrent in the lists provided by the SAs.

This means that, for a limited number of types of processing operations, that will be defined in a harmonised way, all the Supervisory Authorities will require a DPIA to be carried out and the Board will recommend the SAs to amend their lists accordingly in order to ensure consistency.

When this opinion remains silent on DPIA list entries submitted, it means that the Board is not asking the Dutch Supervisory Authority to take further action.

Finally, the Board recalls that transparency is key for data controllers and data processors. In order to clarify the entries in the list, the Board is of the opinion that making an explicit reference in the lists, for each type of processing, to the criteria set out in the guidelines could improve this transparency. Therefore, the Board considers that an explanation on which

criteria have been taken into account by the Dutch Supervisory Authority to create its list could be added.

2.2 Application of the consistency mechanism to the draft list

The submitted draft list by the Dutch Supervisory Authority relates to the offering of goods or services to data subjects, relates to the monitoring of their behaviour in several Member States and/or may substantially affect the free movement of personal data within the Union mainly because the processing operations in the submitted draft list are not limited to data subjects in this country.

2.3 Analysis of the draft list

Taking into account that:

- a. Article 35 (1) GDPR requires a DPIA when the processing activity is likely to result in a high risk to the rights and freedoms of natural persons; and
- b. Article 35 (3) GDPR provides a non-exhaustive list of types of processing that require a DPIA,

the Board is of the opinion that:

BIOMETRIC DATA

The list submitted by the Dutch Supervisory Authority for an opinion of the Board does not currently require a DPIA to be done for the processing of biometric data for the purpose of uniquely identifying a natural person. As such, the Board requests the Dutch Supervisory Authority to amend its list accordingly, by adding explicitly the processing of biometric data for the purpose of uniquely identifying a natural person in conjunction with at least one other criterion to its list, to be applied without prejudice to article 35(3) GDPR.

GENETIC DATA

The list submitted by the Dutch Supervisory Authority for an opinion of the Board envisages that the processing of genetic data, in conjunction with at least one other criterion, requires a DPIA. The Board is of the opinion that the processing of genetic data on its own is not necessarily likely to represent a high risk. However, the processing of genetic data in conjunction with at least one other criterion requires a DPIA to be carried out. The Board takes note of the inclusion of this criterion in the list of Dutch Supervisory Authority.

LOCATION DATA

The Board is of the opinion that the processing of location data on its own is not necessarily likely to represent a high risk. However, the processing of location data in conjunction with at least one other criterion requires a DPIA to be carried out. The list submitted by the Dutch Supervisory Authority for an opinion of the Board does currently in its item 12 require a DPIA to be carried out when there is a processing of location data, in some cases on its own. The Board requests the Dutch Supervisory Authority to amend its list accordingly.

EXCEPTIONS TO INFORMATION TO BE PROVIDED TO THE DATA SUBJECT ACCORDING TO ARTICLE 14.5 GDPR

The Board is of the opinion that types of processing activities that could deprive the data subjects from their rights do not represent a high risk on their own. Therefore, a processing activity conducted by the controller under article 14 GDPR and where the information to be given to the data subjects is subject to an exemption under article 14.5 (b)-(d) could require a DPIA to be carried out only in conjunction with at least one other criterion. The list submitted by the Dutch Supervisory Authority for an opinion of the Board does currently in its item 1 require a DPIA to be done for the processing of data where article 14(5), para (b), (c) and (d) applies, in some cases on its own. The Board requests the Dutch Supervisory Authority to amend its list accordingly.

EMPLOYEE MONITORING

The Board is of the opinion that, due to its specific nature, the employee monitoring processing, meeting the criterion of vulnerable data subjects and of systematic monitoring in the guidelines, – could require a DPIA. Given that the list submitted by the Dutch Supervisory Authority for an opinion of the Board already envisages this type of processing as requiring a data protection impact assessment, the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248. In addition, the Board is of the opinion that the WP249 of the Article 29 working party remains valid when defining the concept of the systematic processing of employee data.

PROCESSING USING NEW/INNOVATIVE TECHNOLOGY

Insofar as item 14 of the list submitted by the Dutch Supervisory Authority for an opinion of the Board envisages that the processing of personal data using innovative technology in conjunction with at least one other criterion], requires a DPIA. The Board takes note of the inclusion of this criterion in the list.

3. Conclusions / Recommendations

The draft list of the Dutch Supervisory Authority may lead to an inconsistent application of the requirement for a DPIA and the following changes need to made:

- Regarding biometric data: the Board requests the Dutch Supervisory Authority to amend its list accordingly, by adding explicitly the processing of biometric data for the purpose of uniquely identifying a natural person in conjunction with at least one other criterion to its list.
- Regarding location data: the Board requests the Dutch Supervisory Authority to amend its list as the processing of location data requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.
- Regarding the exceptions to the information to be given to the data subjects according to article 14.5 GDPR: the Board requests the Dutch Supervisory Authority to amend its list as in this case a DPIA is required only in conjunction with at least one other criterion.

- Regarding employment monitoring: the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248.

4. Final Remarks

This opinion is addressed to the Autoriteit Persoonsgegevens (Dutch Supervisory Authority) and will be made public pursuant to Article 64 (5b) GDPR.

According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 17/2018

on the draft list of the competent supervisory authority of Poland

regarding

**the processing operations subject to the requirement of a data protection
impact assessment (Article 35.4 GDPR)**

Adopted on 25th September 2018

Contents

1.	Summary of the Facts	4
2.	Assessment	5
2.1	General reasoning of the EDPB regarding the submitted list	5
2.2	Application of the consistency mechanism to the draft list	6
2.3	Analysis of the draft list.....	6
	Indicative nature of the list.....	6
	Reference to the Guidelines	6
	Biometric data.....	6
	Genetic data.....	7
	Location data	7
	Employee Monitoring	7
	Inconsistency with the Guidelines	7
	Processing using new/innovative technology	7
3.	Conclusions / Recommendations	8
4.	Final Remarks.....	8

The European Data Protection Board

Having regard to Article 63, Article 64 (1a), (3) - (8) and Article 35 (1), (3), (4), (6) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (here after GDPR) throughout the European Economic Area. In compliance with article 64.1 GDPR, the Board has to issue an opinion where a supervisory authority intends to adopt a list of processing operations subject to the requirement for a data protection impact assessment pursuant to article 35.4 GDPR. The aim of this opinion is therefore to create a harmonized approach with regard to processing that is cross border or that can affect the free flow of personal data or natural person across the European Union. Even though the GDPR doesn't impose a single list, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by requesting SAs to include some types of processing in their lists, secondly by requesting them to remove some criteria which the Board doesn't consider as necessarily creating high risks for data subjects, and finally by requesting them to use some criteria in a harmonized manner.

(2) With reference to Article 35 (4) and (6) GDPR, the competent supervisory authorities shall establish lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment (hereinafter "DPIA"). They shall, however, apply the consistency mechanism where such lists involve processing operations, which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

(3) While the draft lists of the competent supervisory authorities are subject to the consistency mechanism, this does not mean that the lists should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB assessment/opinion is not to reach a single EU list but rather to avoid significant inconsistencies that may affect the equivalent protection of the data subjects.

(4) The carrying out of a DPIA is only mandatory for the controller pursuant to Article 35 (1) GDPR where processing is "likely to result in a high risk to the rights and freedoms of natural

persons". Article 35 (3) GDPR illustrates what is likely to result in a high risk. This is a non-exhaustive list. The Working Party 29 in the Guidelines on data protection impact assessment¹, as endorsed by the EDPB², has clarified criteria that can help to identify when processing operations are subject to the requirement for a DPIA. The Working Party 29 Guidelines WP248 state that in most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out, however, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

(5) The lists produced by the competent supervisory authorities support the same objective to identify processing operations likely to result in a high risk and processing operations, which therefore require a DPIA. As such, the criteria developed in the Working Party 29 Guidelines should be applied when assessing whether the draft lists of the competent supervisory authorities does not affect the consistent application of the GDPR.

(6) Twenty-two competent supervisory authorities have submitted their draft lists to the EDPB. A global assessment of these draft lists supports the objective of a consistent application of the GDPR even though the complexity of the subject matter increases.

(7) The opinion of the EDPB shall be adopted pursuant to Article 64 (3) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

I. Summary of the Facts

The Urząd Ochrony Danych Osobowych (hereafter Polish Supervisory Authority) has submitted its draft list to the EDPB. The decision on the completeness of the file was taken on 20th of June 2018. This period until which the opinion to be adopted has been extended until the 25th of September taking into account the complexity of the subject matter considering that at the same time twenty-two competent supervisory authorities submitted the draft lists and thus the need for a global assessment arose.

¹ WP29, Guidelines on Data Protection Impact Assessment and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP 248 rev. 01).

² EDPB, Endorsement 1/2018.

2. Assessment

2.1 General reasoning of the EDPB regarding the submitted list

Any list submitted to the EDPB has been interpreted as further specifying Art 35.1, which will prevail in any case. Thus, no list can be exhaustive. As the list provided by Polish Supervisory Authority does not explicitly state this, the Board requests this explanation to be added to the document containing the list.

In compliance with article 35.10 GDPR, the Board is of the opinion that if a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of the legal basis the obligation to carry out a DPIA in accordance with paragraphs 1 to 7 of article 35 GDPR does not apply, unless the Member State deems it necessary.

Further, if the Board requests a DPIA for a certain category of processing and an equivalent measure is already required by national law, the Polish Supervisory Authority shall add a reference to this measure.

This opinion does not reflect upon items submitted by the Polish Supervisory Authority, which were deemed outside the scope of Article 35.6 GDPR. This refers to items that neither relate "to the offering of goods or services to data subjects" in several Member States nor to the monitoring of the behaviour of data subjects in several Member States. Additionally, they are not likely to "substantially affect the free movement of personal data within the Union". This is especially the case for items relating to national legislation and in particular where the obligation to carry out a DPIA is stipulated in national legislation. Further, any processing operations that relate to law enforcement were deemed out of scope, as they are not in scope of the GDPR.

The Board has noted that several supervisory authorities have included in their lists some types of processing which are necessarily local processing. Given that only cross border processing and processing that may affect the free flow of personal data and data subjects are concerned by Article 35.6, the Board will not comment on those local processing.

The opinion aims at defining a consistent core of processing operations that are recurrent in the lists provided by the SAs.

This means that, for a limited number of types of processing operations, that will be defined in a harmonised way, all the Supervisory Authorities will require a DPIA to be carried out and the Board will recommend the SAs to amend their lists accordingly in order to ensure consistency.

When this opinion remains silent on DPIA list entries submitted, it means that the Board is not asking the Polish Supervisory Authority to take further action.

Finally, the Board recalls that transparency is key for data controllers and data processors. In order to clarify the entries in the list, the Board is of the opinion that making an explicit

reference in the lists, for each type of processing, to the criteria set out in the guidelines could improve this transparency. Therefore, the Board considers that an explanation on which criteria have been taken into account by the Polish Supervisory Authority to create its list could be added.

2.2 Application of the consistency mechanism to the draft list

The submitted draft list by the Polish Supervisory Authority relates to the offering of goods or services to data subjects, relates to the monitoring of their behaviour in several Member States and/or may substantially affect the free movement of personal data within the Union mainly because the processing operations in the submitted draft list are not limited to data subjects in this country.

2.3 Analysis of the draft list

Taking into account that:

- a. Article 35 (1) GDPR requires a DPIA when the processing activity is likely to result in a high risk to the rights and freedoms of natural persons; and
- b. Article 35 (3) GDPR provides a non-exhaustive list of types of processing that require a DPIA,

the Board is of the opinion that:

INDICATIVE NATURE OF THE LIST

As the list provided by Polish Supervisory Authority does not explicitly state that its list is not exhaustive, the Board requests this explanation to be added to the document containing the list.

REFERENCE TO THE GUIDELINES

The board is of the opinion that the analysis done in the Working Party 29 Guidelines WP248 are a core element for ensuring consistency across the Union. Thus, it requests the different Supervisor Authorities to add a statement to the document containing their list that clarifies that their list is based on these guidelines and that it complements and further specifies the guidelines.

As the document of the Polish Supervisory Authority does not contain such a statement, the Board recommends the Polish Supervisory Authority to amend its document accordingly.

BIOMETRIC DATA

The list submitted by the Polish Supervisory Authority for an opinion of the Board does not currently require a DPIA to be done for the processing of biometric data for the purpose of uniquely identifying a natural person. As such, the Board requests the Polish Supervisory Authority to amend its list accordingly, by adding explicitly the processing of biometric data for the purpose of uniquely identifying a natural person in conjunction with at least one other criterion to its list, to be applied without prejudice to article 35(3) GDPR.

GENETIC DATA

The list submitted by the Polish Supervisory Authority for an opinion of the Board does not currently require a DPIA to be done for the processing of genetic data. . The Board is of the opinion that the processing of genetic data on its own is not necessarily likely to represent a high risk. However, the processing of genetic data in conjunction with at least one other criterion requires a DPIA to be carried out. As such, the Board requests the Polish Supervisory Authority to amend its list accordingly, by adding explicitly the processing of genetic data in conjunction with at least one other criterion to its list, to be applied without prejudice to article 35(3) GDPR.

LOCATION DATA

The Board is of the opinion that consistency is one of the basic principle of the GDPR. The Board notes that a majority of the lists submitted explicitly contain a reference to the processing of location data. As the list submitted by the Polish Supervisory Authority for an opinion do not contain such a reference, the Board encourages the Polish Supervisory Authority to include the processing of location data in its list, together with another criterion.

EMPLOYEE MONITORING

The Board is of the opinion that, due to its specific nature, the employee monitoring processing, meeting the criterion of vulnerable data subjects and of systematic monitoring in the guidelines, – could require a DPIA. Given that the list submitted by the Polish Supervisory Authority for an opinion of the Board already envisages this type of processing as requiring a data protection impact assessment, the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248. In addition, the Board is of the opinion that the WP249 of the Article 29 working party remains valid when defining the concept of the systematic processing of employee data.

INCONSISTENCY WITH THE GUIDELINES

The Board noticed that the Polish Supervisory Authority repeats the criteria of the Working Party 29 Guidelines in its items 2, 4, 5, 6, 8 and 9. However, the Guidelines state that in most cases a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out. As such, the Board is of the opinion that the list submitted by the Polish Supervisory Authority is not in line with the guidelines. Therefore the Board requests the Polish Supervisory Authority to bring its list in compliance with the guidelines by adding the fact that, in most cases, for the aforementioned points, only a processing meeting two criteria would require a DPIA, and that the more criteria are met by the processing, the more likely it is to present a high risk to the rights and freedoms of data subjects, and therefore to require a DPIA, regardless of the measures which the controller envisages to adopt.

PROCESSING USING NEW/INNOVATIVE TECHNOLOGY

The list submitted by the Polish Supervisory Authority for an opinion of the Board envisages that the processing of personal data using innovative technology in conjunction with at least one other criterion, requires a DPIA. The Board takes note of the inclusion of this criterion in the list.

3. Conclusions / Recommendations

The draft list of the Polish Supervisory Authority may lead to an inconsistent application of the requirement for a DPIA and the following changes need to made:

- Regarding the indicative nature of the list: the Board requests an explanation to be added to the document containing the list, stating its non-exhaustive nature.
- Regarding the reference to the guidelines: the Board requests the Polish Supervisory Authority to amend its document accordingly.
- Regarding biometric data: the Board requests the Polish Supervisory Authority to amend its list accordingly, by adding explicitly the processing of biometric data for the purpose of uniquely identifying a natural person in conjunction with at least one other criterion to its list.
- Regarding genetic data: the Board requests the Polish Supervisory Authority to amend its list by adding explicitly the processing of genetic data in conjunction with at least one other criterion to its list.
- Regarding location data: the Board encourages the Polish Supervisory Authority to include the processing of location data in its list, together with another criterion.
- Regarding employment monitoring: the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248.
- Regarding the inconsistency with the Guidelines: the Board requests the Polish Supervisory Authority to bring its list in compliance with the guidelines by adding the fact that, in most cases, for the aforementioned points, only a processing meeting two criteria would require a DPIA.

4. Final Remarks

This opinion is addressed to the Urząd Ochrony Danych Osobowych (Polish Supervisory Authority) and will be made public pursuant to Article 64 (5b) GDPR.

According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 18/2018

on the draft list of the competent supervisory authority of Portugal

regarding

**the processing operations subject to the requirement of a data protection
impact assessment (Article 35.4 GDPR)**

Adopted on 25th September 2018

Contents

1.	Summary of the Facts	4
2.	Assessment	5
2.1	General reasoning of the EDPB regarding the submitted list	5
2.2	Application of the consistency mechanism to the draft list	6
2.3	Analysis of the draft list.....	6
	Reference to the Guidelines	6
	Biometric data.....	6
	Genetic data.....	6
	Location data	7
	Processing for scientific or historical purposes without consent	7
	Further processing	7
	Exceptions to information to be provided to the data subject according to article 14.5 GDPR	7
	Employee Monitoring	8
	Processing carried out with the aid of an implant.....	8
	Interfaces of personal electronic Device unprotected against unauthorized readout	8
	Processing using new/innovative technology	8
3.	Conclusions / Recommendations	9
4.	Final Remarks	10

The European Data Protection Board

Having regard to Article 63, Article 64 (1a), (3) - (8) and Article 35 (1), (3), (4), (6) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (here after GDPR) throughout the European Economic Area. In compliance with article 64.1 GDPR, the Board has to issue an opinion where a supervisory authority intends to adopt a list of processing operations subject to the requirement for a data protection impact assessment pursuant to article 35.4 GDPR. The aim of this opinion is therefore to create a harmonized approach with regard to processing that is cross border or that can affect the free flow of personal data or natural person across the European Union. Even though the GDPR doesn't impose a single list, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by requesting SAs to include some types of processing in their lists, secondly by requesting them to remove some criteria which the Board doesn't consider as necessarily creating high risks for data subjects, and finally by requesting them to use some criteria in a harmonized manner.

(2) With reference to Article 35 (4) and (6) GDPR, the competent supervisory authorities shall establish lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment (hereinafter "DPIA"). They shall, however, apply the consistency mechanism where such lists involve processing operations, which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

(3) While the draft lists of the competent supervisory authorities are subject to the consistency mechanism, this does not mean that the lists should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB assessment/opinion is not to reach a single EU list but rather to avoid significant inconsistencies that may affect the equivalent protection of the data subjects.

(4) The carrying out of a DPIA is only mandatory for the controller pursuant to Article 35 (1) GDPR where processing is "likely to result in a high risk to the rights and freedoms of natural

persons". Article 35 (3) GDPR illustrates what is likely to result in a high risk. This is a non-exhaustive list. The Working Party 29 in the Guidelines on data protection impact assessment¹, as endorsed by the EDPB², has clarified criteria that can help to identify when processing operations are subject to the requirement for a DPIA. The Working Party 29 Guidelines WP248 state that in most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out, however, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

(5) The lists produced by the competent supervisory authorities support the same objective to identify processing operations likely to result in a high risk and processing operations, which therefore require a DPIA. As such, the criteria developed in the Working Party 29 Guidelines should be applied when assessing whether the draft lists of the competent supervisory authorities does not affect the consistent application of the GDPR.

(6) Twenty-two competent supervisory authorities have submitted their draft lists to the EDPB. A global assessment of these draft lists supports the objective of a consistent application of the GDPR even though the complexity of the subject matter increases.

(7) The opinion of the EDPB shall be adopted pursuant to Article 64 (3) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

I. Summary of the Facts

The Comissão Nacional de Protecção de Dados - CNPD (hereafter Portuguese Supervisory Authority) has submitted its draft list to the EDPB. The decision on the completeness of the file was taken on 10th of July 2018. This period until which the opinion to be adopted has been extended until the 25th of September taking into account the complexity of the subject matter considering that at the same time twenty-two competent supervisory authorities submitted the draft lists and thus the need for a global assessment arose.

¹ WP29, Guidelines on Data Protection Impact Assessment and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP 248 rev. 01).

² EDPB, Endorsement 1/2018.

2. Assessment

2.1 General reasoning of the EDPB regarding the submitted list

Any list submitted to the EDPB has been interpreted as further specifying Art 35.1, which will prevail in any case. Thus, no list can be exhaustive.

In compliance with article 35.10 GDPR, the Board is of the opinion that if a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of the legal basis the obligation to carry out a DPIA in accordance with paragraphs 1 to 7 of article 35 GDPR does not apply, unless the Member State deems it necessary.

Further, if the Board requests a DPIA for a certain category of processing and an equivalent measure is already required by national law, the Portuguese Supervisory Authority shall add a reference to this measure.

This opinion does not reflect upon items submitted by the Portuguese Supervisory Authority, which were deemed outside the scope of Article 35.6 GDPR. This refers to items that neither relate “to the offering of goods or services to data subjects” in several Member States nor to the monitoring of the behaviour of data subjects in several Member States. Additionally, they are not likely to “substantially affect the free movement of personal data within the Union”. This is especially the case for items relating to national legislation and in particular where the obligation to carry out a DPIA is stipulated in national legislation. Further, any processing operations that relate to law enforcement were deemed out of scope, as they are not in scope of the GDPR.

The Board has noted that several supervisory authorities have included in their lists some types of processing which are necessarily local processing. Given that only cross border processing and processing that may affect the free flow of personal data and data subjects are concerned by Article 35.6, the Board will not comment on those local processing.

The opinion aims at defining a consistent core of processing operations that are recurrent in the lists provided by the SAs.

This means that, for a limited number of types of processing operations, that will be defined in a harmonised way, all the Supervisory Authorities will require a DPIA to be carried out and the Board will recommend the SAs to amend their lists accordingly in order to ensure consistency.

When this opinion remains silent on DPIA list entries submitted, it means that the Board is not asking the Portuguese Supervisory Authority to take further action.

Finally, the Board recalls that transparency is key for data controllers and data processors. In order to clarify the entries in the list, the Board is of the opinion that making an explicit reference in the lists, for each type of processing, to the criteria set out in the guidelines could improve this transparency. Therefore, the Board considers that an explanation on which

criteria have been taken into account by the Portuguese Supervisory Authority to create its list could be added.

2.2 Application of the consistency mechanism to the draft list

The submitted draft list by the Portuguese Supervisory Authority relates to the offering of goods or services to data subjects, relates to the monitoring of their behaviour in several Member States and/or may substantially affect the free movement of personal data within the Union mainly because the processing operations in the submitted draft list are not limited to data subjects in this country.

2.3 Analysis of the draft list

Taking into account that:

- a. Article 35 (1) GDPR requires a DPIA when the processing activity is likely to result in a high risk to the rights and freedoms of natural persons; and
- b. Article 35 (3) GDPR provides a non-exhaustive list of types of processing that require a DPIA,

the Board is of the opinion that:

REFERENCE TO THE GUIDELINES

The board is of the opinion that the analysis done in the Working Party 29 Guidelines WP248 are a core element for ensuring consistency across the Union. Thus, it requests the different Supervisor Authorities to add a statement to the document containing their list that clarifies that their list is based on these guidelines and that it complements and further specifies the guidelines.

As the document of the Portuguese Supervisory Authority does not contain such a statement, the Board recommends the Portuguese Supervisory Authority to amend its document accordingly.

BIOMETRIC DATA

The list submitted by the Portuguese Supervisory Authority for an opinion of the Board states, that the processing of biometric data falls under the obligation to perform a DPIA on its own. The Board is of the opinion that the processing of biometric data on its own is not necessarily likely to represent a high risk. However, the processing of biometric data for the purpose of uniquely identifying a natural person in conjunction with at least one other criterion requires a DPIA to be carried out. As such, the Board requests the Portuguese Supervisory Authority to amend its list accordingly, by adding that the item referencing the processing of biometric data for the purpose of uniquely identifying a natural person requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion, to be applied without prejudice to article 35(3) GDPR.

GENETIC DATA

The list submitted by the Portuguese Supervisory Authority for an opinion of the Board does not currently require a DPIA to be done for the processing of genetic data. The Board is of the

opinion that the processing of genetic data on its own is not necessarily likely to represent a high risk. However, the processing of genetic data in conjunction with at least one other criterion requires a DPIA to be carried out. As such, the Board requests the Portuguese Supervisory Authority to amend its list accordingly, by adding explicitly the processing of genetic data in conjunction with at least one other criterion to its list, to be applied without prejudice to article 35(3) GDPR.

LOCATION DATA

The Board is of the opinion that the processing of location data on its own is not necessarily likely to represent a high risk. However, the processing of location data in conjunction with at least one other criterion requires a DPIA to be carried out. The list submitted by the Portuguese Supervisory Authority for an opinion of the Board does currently require a DPIA to be carried out when there is a processing of location data on its own. The Board requests the Portuguese Supervisory Authority to amend its list accordingly, by adding that the item referencing the processing of location data requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.

PROCESSING FOR SCIENTIFIC OR HISTORICAL PURPOSES WITHOUT CONSENT

The Board is of the opinion that the processing of personal data for scientific or historical purposes on its own is not necessarily likely to represent a high risk. However, the processing of personal data for scientific or historical purpose in conjunction with at least one other criterion does require a DPIA to be carried out. The list submitted by the Portuguese Supervisory Authority for an opinion of the Board states that this type of processing in conjunction with at least one other criterion falls under the obligation to perform a DPIA. The Board takes note of the inclusion of this criterion in the list.

FURTHER PROCESSING

The Board is of the opinion that further processing of personal data should not be a criterion leading to an obligation to do a DPIA, alone or with another criterion. The list submitted by the Portuguese Supervisory Authority for an opinion of the Board does currently require a DPIA to be carried out for the further processing of personal data. The Board requests the Portuguese Supervisory Authority to amend its list accordingly, by removing this criterion.

EXCEPTIONS TO INFORMATION TO BE PROVIDED TO THE DATA SUBJECT ACCORDING TO ARTICLE 14.5 GDPR

The Board is of the opinion that types of processing activities that could deprive the data subjects from their rights do not represent a high risk on their own. Therefore, a processing activity conducted by the controller under article 14 GDPR and where the information to be given to the data subjects is subject to an exemption under article 14.5 (b)-(d) could require a DPIA to be carried out only in conjunction with at least one other criterion. The list submitted by the Portuguese Supervisory Authority for an opinion of the Board does currently require a DPIA to be done for the processing of data where article 14(5), para (b), (c) and (d) applies on its own. The Board requests the Portuguese Supervisory Authority to amend its list

accordingly, by adding that it requires a DPIA only in conjunction with at least one other criterion.

EMPLOYEE MONITORING

The Board is of the opinion that, due to its specific nature, the employee monitoring processing, meeting the criterion of vulnerable data subjects and of systematic monitoring in the guidelines, – could require a DPIA. Given that the list submitted by the Portuguese Supervisory Authority for an opinion of the Board already envisages this type of processing as requiring a data protection impact assessment, the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248. In addition, the Board is of the opinion that the WP249 of the Article 29 working party remains valid when defining the concept of the systematic processing of employee data.

PROCESSING CARRIED OUT WITH THE AID OF AN IMPLANT

The Board is of the opinion that, the processing of non-health data with the aid of an implant does not require a DPIA in every instance. The list submitted by the Portuguese Supervisory Authority for an opinion of the Board does currently not clarify that a DPIA is to be done for the processing of health data with the aid of an implant. As such, the Board requests the Portuguese Supervisory Authority to amend its list accordingly, by stating that in any event the processing of health data with the aid of an implant requires a DPIA to be carried out.

INTERFACES OF PERSONAL ELECTRONIC DEVICE UNPROTECTED AGAINST UNAUTHORIZED READOUT

The Board is of the opinion that the processing made in the context of the collection of personal data via interfaces of personal electronic devices, which are not protected against unauthorized readout, should not be a criterion leading to an obligation to do a DPIA, alone or with another criterion. Given that the list submitted by the Portuguese Supervisory Authority for an opinion of the Board envisages this type of processing as requiring a data protection impact assessment in its item 2, the Board requests the Portuguese Supervisory Authority to amend its list accordingly.

PROCESSING USING NEW/INNOVATIVE TECHNOLOGY

The list submitted by the Portuguese Supervisory Authority for an opinion of the Board envisages that the use of new or innovative technology, on its own, requires a DPIA. The Board is of the opinion that the use of innovative technology on its own is not necessarily likely to represent a high risk. However, the use of innovative technology in conjunction with at least one other criterion requires a DPIA to be carried out. Therefore, the Board requests the Portuguese Supervisory Authority to amend its list accordingly, firstly by referring in their list to innovative technology and secondly by adding that the item requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.

3. Conclusions / Recommendations

The draft list of the Portuguese Supervisory Authority may lead to an inconsistent application of the requirement for a DPIA and the following changes need to made:

- Regarding the reference to the guidelines: the Board requests the Portuguese Supervisory Authority to amend its document accordingly.
- Regarding biometric data: the Board requests the Portuguese Supervisory Authority to amend its list by adding that the item referencing the processing of biometric data for the purpose of uniquely identifying a natural person requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.
- Regarding genetic data: the Board requests the Portuguese Supervisory Authority to amend its list by adding explicitly the processing of genetic data in conjunction with at least one other criterion to its list.
- Regarding location data: the Board requests the Portuguese Supervisory Authority to amend its list by adding that the item referencing the processing of location data requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.
- Regarding further processing: the Board requests the Portuguese Supervisory Authority to amend its list accordingly, by removing this criterion.
- Regarding the exceptions to the information to be given to the data subjects according to article 14.5 GDPR: the Board requests the Portuguese Supervisory Authority to amend its list by adding that it requires a DPIA only in conjunction with at least one other criterion
- Regarding employment monitoring: the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248.
- Regarding processing carried out with the aid of an implant: the Board requests the Portuguese Supervisory Authority to amend its list by stating that only the processing of health data with the aid of an implant requires a DPIA to be carried out.
- Regarding interfaces of personal electronic devices unprotected against unauthorized readout: the Board requests the Portuguese Supervisory Authority to amend its list by removing the reference to the collection of personal data via interfaces of personal electronic devices which are not protected against unauthorized readout from its list.
- Regarding processing using new or innovative technology: the Board requests the Portuguese Supervisory Authority to amend its list firstly by referring in their list to innovative technology and secondly by adding that the item requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.

4. Final Remarks

This opinion is addressed to the Comissão Nacional de Protecção de Dados - CNPD (Portuguese Supervisory Authority) and will be made public pursuant to Article 64 (5b) GDPR.

According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 19/2018

on the draft list of the competent supervisory authority of Romania

regarding

**the processing operations subject to the requirement of a data protection
impact assessment (Article 35.4 GDPR)**

Adopted on 25th September 2018

Contents

1.	Summary of the Facts	4
2.	Assessment	5
2.1	General reasoning of the EDPB regarding the submitted list	5
2.2	Application of the consistency mechanism to the draft list	6
2.3	Analysis of the draft list.....	6
	Indicative nature of the list.....	6
	Reference to the Guidelines	6
	Biometric data.....	6
	Genetic data.....	7
	Employee Monitoring	7
	Processing using new/innovative technology	7
3.	Conclusions / Recommendations	7
4.	Final Remarks.....	8

The European Data Protection Board

Having regard to Article 63, Article 64 (1a), (3) - (8) and Article 35 (1), (3), (4), (6) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (here after GDPR) throughout the European Economic Area. In compliance with article 64.1 GDPR, the Board has to issue an opinion where a supervisory authority intends to adopt a list of processing operations subject to the requirement for a data protection impact assessment pursuant to article 35.4 GDPR. The aim of this opinion is therefore to create a harmonized approach with regard to processing that is cross border or that can affect the free flow of personal data or natural person across the European Union. Even though the GDPR doesn't impose a single list, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by requesting SAs to include some types of processing in their lists, secondly by requesting them to remove some criteria which the Board doesn't consider as necessarily creating high risks for data subjects, and finally by requesting them to use some criteria in a harmonized manner.

(2) With reference to Article 35 (4) and (6) GDPR, the competent supervisory authorities shall establish lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment (hereinafter "DPIA"). They shall, however, apply the consistency mechanism where such lists involve processing operations, which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

(3) While the draft lists of the competent supervisory authorities are subject to the consistency mechanism, this does not mean that the lists should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB assessment/opinion is not to reach a single EU list but rather to avoid significant inconsistencies that may affect the equivalent protection of the data subjects.

(4) The carrying out of a DPIA is only mandatory for the controller pursuant to Article 35 (1) GDPR where processing is "likely to result in a high risk to the rights and freedoms of natural

persons". Article 35 (3) GDPR illustrates what is likely to result in a high risk. This is a non-exhaustive list. The Working Party 29 in the Guidelines on data protection impact assessment¹, as endorsed by the EDPB², has clarified criteria that can help to identify when processing operations are subject to the requirement for a DPIA. The Working Party 29 Guidelines WP248 state that in most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out, however, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

(5) The lists produced by the competent supervisory authorities support the same objective to identify processing operations likely to result in a high risk and processing operations, which therefore require a DPIA. As such, the criteria developed in the Working Party 29 Guidelines should be applied when assessing whether the draft lists of the competent supervisory authorities does not affect the consistent application of the GDPR.

(6) Twenty-two competent supervisory authorities have submitted their draft lists to the EDPB. A global assessment of these draft lists supports the objective of a consistent application of the GDPR even though the complexity of the subject matter increases.

(7) The opinion of the EDPB shall be adopted pursuant to Article 64 (3) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

I. Summary of the Facts

The Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (hereafter Romanian Supervisory Authority) has submitted its draft list to the EDPB. The decision on the completeness of the file was taken on 10th of July 2018. This period until which the opinion to be adopted has been extended until the 25th of September taking into account the complexity of the subject matter considering that at the same time twenty-two competent supervisory authorities submitted the draft lists and thus the need for a global assessment arose.

¹ WP29, Guidelines on Data Protection Impact Assessment and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP 248 rev. 01).

² EDPB, Endorsement 1/2018.

2. Assessment

2.1 General reasoning of the EDPB regarding the submitted list

Any list submitted to the EDPB has been interpreted as further specifying Art 35.1, which will prevail in any case. Thus, no list can be exhaustive. As the list provided by Romanian Supervisory Authority does not explicitly state this, the Board requests this explanation to be added to the document containing the list.

In compliance with article 35.10 GDPR, the Board is of the opinion that if a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of the legal basis the obligation to carry out a DPIA in accordance with paragraphs 1 to 7 of article 35 GDPR does not apply, unless the Member State deems it necessary.

Further, if the Board requests a DPIA for a certain category of processing and an equivalent measure is already required by national law, the Romanian Supervisory Authority shall add a reference to this measure.

This opinion does not reflect upon items submitted by the Romanian Supervisory Authority, which were deemed outside the scope of Article 35.6 GDPR. This refers to items that neither relate “to the offering of goods or services to data subjects” in several Member States nor to the monitoring of the behaviour of data subjects in several Member States. Additionally, they are not likely to “substantially affect the free movement of personal data within the Union”. This is especially the case for items relating to national legislation and in particular where the obligation to carry out a DPIA is stipulated in national legislation. Further, any processing operations that relate to law enforcement were deemed out of scope, as they are not in scope of the GDPR.

The Board has noted that several supervisory authorities have included in their lists some types of processing which are necessarily local processing. Given that only cross border processing and processing that may affect the free flow of personal data and data subjects are concerned by Article 35.6, the Board will not comment on those local processing.

The opinion aims at defining a consistent core of processing operations that are recurrent in the lists provided by the SAs.

This means that, for a limited number of types of processing operations, that will be defined in a harmonised way, all the Supervisory Authorities will require a DPIA to be carried out and the Board will recommend the SAs to amend their lists accordingly in order to ensure consistency.

When this opinion remains silent on DPIA list entries submitted, it means that the Board is not asking the Romanian Supervisory Authority to take further action.

Finally, the Board recalls that transparency is key for data controllers and data processors. In order to clarify the entries in the list, the Board is of the opinion that making an explicit

reference in the lists, for each type of processing, to the criteria set out in the guidelines could improve this transparency. Therefore, the Board considers that an explanation on which criteria have been taken into account by the Romanian Supervisory Authority to create its list could be added.

2.2 Application of the consistency mechanism to the draft list

The submitted draft list by the Romanian Supervisory Authority relates to the offering of goods or services to data subjects, relates to the monitoring of their behaviour in several Member States and/or may substantially affect the free movement of personal data within the Union mainly because the processing operations in the submitted draft list are not limited to data subjects in this country.

2.3 Analysis of the draft list

Taking into account that:

- a. Article 35 (1) GDPR requires a DPIA when the processing activity is likely to result in a high risk to the rights and freedoms of natural persons; and
- b. Article 35 (3) GDPR provides a non-exhaustive list of types of processing that require a DPIA,

the Board is of the opinion that:

INDICATIVE NATURE OF THE LIST

As the list provided by Romanian Supervisory Authority does not explicitly state that its list is not exhaustive, the Board requests this explanation to be added to the document containing the list.

REFERENCE TO THE GUIDELINES

The board is of the opinion that the analysis done in the Working Party 29 Guidelines WP248 are a core element for ensuring consistency across the Union. Thus, it requests the different Supervisor Authorities to add a statement to the document containing their list that clarifies that their list is based on these guidelines and that it complements and further specifies the guidelines.

As the document of the Romanian Supervisory Authority does not contain such a statement, the Board recommends the Romanian Supervisory Authority to amend its document accordingly.

BIOMETRIC DATA

The list submitted by the Romanian Supervisory Authority for an opinion of the Board envisages that the processing of biometric data for the purpose of uniquely identifying a natural person, in conjunction with at least one other criterion, requires a DPIA. On this point, the Board acknowledges that the list aligns with the aim of consistency.

GENETIC DATA

The list submitted by the Romanian Supervisory Authority for an opinion of the Board envisages that the processing of genetic data, in conjunction with at least one other criterion, requires a DPIA. The Board is of the opinion that the processing of genetic data on its own is not necessarily likely to represent a high risk. However, the processing of genetic data in conjunction with at least one other criterion requires a DPIA to be carried out. The Board takes note of the inclusion of this criterion in the list of Romanian Supervisory Authority.

EMPLOYEE MONITORING

The Board is of the opinion that, due to its specific nature, the employee monitoring processing, meeting the criterion of vulnerable data subjects and of systematic monitoring in the guidelines, – could require a DPIA. Given that the list submitted by the Romanian Supervisory Authority for an opinion of the Board already envisages this type of processing as requiring a data protection impact assessment, the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248. In addition, the Board is of the opinion that the WP249 of the Article 29 working party remains valid when defining the concept of the systematic processing of employee data.

PROCESSING USING NEW/INNOVATIVE TECHNOLOGY

The list submitted by the Romanian Supervisory Authority for an opinion of the Board envisages that the processing of personal data using innovative technology in conjunction with at least one other criterion, requires a DPIA. The Board takes note of the inclusion of this criterion in the list.

3. Conclusions / Recommendations

The draft list of the Romanian Supervisory Authority may lead to an inconsistent application of the requirement for a DPIA and the following changes need to made:

- Regarding the indicative nature of the list: the Board requests an explanation to be added to the document containing the list, stating its non-exhaustive nature.
- Regarding the reference to the guidelines: the Board requests the Romanian Supervisory Authority to amend its document accordingly.
- Regarding employment monitoring: the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248.

4. Final Remarks

This opinion is addressed to the Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (Romanian Supervisory Authority) and will be made public pursuant to Article 64 (5b) GDPR.

According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 20/2018

on the draft list of the competent supervisory authority of Sweden

regarding

**the processing operations subject to the requirement of a data protection
impact assessment (Article 35.4 GDPR)**

Adopted on 25th September 2018

Contents

1.	Summary of the Facts	4
2.	Assessment	5
2.1	General reasoning of the EDPB regarding the submitted list	5
2.2	Application of the consistency mechanism to the draft list	6
2.3	Analysis of the draft list.....	6
	Reference to the Guidelines	6
	Biometric data.....	6
	Genetic data.....	6
	Employee Monitoring	7
	Processing using new/innovative technology	7
3.	Conclusions / Recommendations	7
4.	Final Remarks	7

The European Data Protection Board

Having regard to Article 63, Article 64 (1a), (3) - (8) and Article 35 (1), (3), (4), (6) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (here after GDPR) throughout the European Economic Area. In compliance with article 64.1 GDPR, the Board has to issue an opinion where a supervisory authority intends to adopt a list of processing operations subject to the requirement for a data protection impact assessment pursuant to article 35.4 GDPR. The aim of this opinion is therefore to create a harmonized approach with regard to processing that is cross border or that can affect the free flow of personal data or natural person across the European Union. Even though the GDPR doesn't impose a single list, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by requesting SAs to include some types of processing in their lists, secondly by requesting them to remove some criteria which the Board doesn't consider as necessarily creating high risks for data subjects, and finally by requesting them to use some criteria in a harmonized manner.

(2) With reference to Article 35 (4) and (6) GDPR, the competent supervisory authorities shall establish lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment (hereinafter "DPIA"). They shall, however, apply the consistency mechanism where such lists involve processing operations, which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

(3) While the draft lists of the competent supervisory authorities are subject to the consistency mechanism, this does not mean that the lists should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB assessment/opinion is not to reach a single EU list but rather to avoid significant inconsistencies that may affect the equivalent protection of the data subjects.

(4) The carrying out of a DPIA is only mandatory for the controller pursuant to Article 35 (1) GDPR where processing is "likely to result in a high risk to the rights and freedoms of natural

persons". Article 35 (3) GDPR illustrates what is likely to result in a high risk. This is a non-exhaustive list. The Working Party 29 in the Guidelines on data protection impact assessment¹, as endorsed by the EDPB², has clarified criteria that can help to identify when processing operations are subject to the requirement for a DPIA. The Working Party 29 Guidelines WP248 state that in most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out, however, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

(5) The lists produced by the competent supervisory authorities support the same objective to identify processing operations likely to result in a high risk and processing operations, which therefore require a DPIA. As such, the criteria developed in the Working Party 29 Guidelines should be applied when assessing whether the draft lists of the competent supervisory authorities does not affect the consistent application of the GDPR.

(6) Twenty-two competent supervisory authorities have submitted their draft lists to the EDPB. A global assessment of these draft lists supports the objective of a consistent application of the GDPR even though the complexity of the subject matter increases.

(7) The opinion of the EDPB shall be adopted pursuant to Article 64 (3) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

I. Summary of the Facts

The Datainspektionen (hereafter Swedish Supervisory Authority) has submitted its draft list to the EDPB. The decision on the completeness of the file was taken on 11th of July 2018. This period until which the opinion to be adopted has been extended until the 25th of September taking into account the complexity of the subject matter considering that at the same time twenty-two competent supervisory authorities submitted the draft lists and thus the need for a global assessment arose.

¹ WP29, Guidelines on Data Protection Impact Assessment and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP 248 rev. 01).

² EDPB, Endorsement 1/2018.

2. Assessment

2.1 General reasoning of the EDPB regarding the submitted list

Any list submitted to the EDPB has been interpreted as further specifying Art 35.1, which will prevail in any case. Thus, no list can be exhaustive.

In compliance with article 35.10 GDPR, the Board is of the opinion that if a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of the legal basis the obligation to carry out a DPIA in accordance with paragraphs 1 to 7 of article 35 GDPR does not apply, unless the Member State deems it necessary.

Further, if the Board requests a DPIA for a certain category of processing and an equivalent measure is already required by national law, the Swedish Supervisory Authority shall add a reference to this measure.

This opinion does not reflect upon items submitted by the Swedish Supervisory Authority, which were deemed outside the scope of Article 35.6 GDPR. This refers to items that neither relate “to the offering of goods or services to data subjects” in several Member States nor to the monitoring of the behaviour of data subjects in several Member States. Additionally, they are not likely to “substantially affect the free movement of personal data within the Union”. This is especially the case for items relating to national legislation and in particular where the obligation to carry out a DPIA is stipulated in national legislation. Further, any processing operations that relate to law enforcement were deemed out of scope, as they are not in scope of the GDPR.

The Board has noted that several supervisory authorities have included in their lists some types of processing which are necessarily local processing. Given that only cross border processing and processing that may affect the free flow of personal data and data subjects are concerned by Article 35.6, the Board will not comment on those local processing.

The opinion aims at defining a consistent core of processing operations that are recurrent in the lists provided by the SAs.

This means that, for a limited number of types of processing operations, that will be defined in a harmonised way, all the Supervisory Authorities will require a DPIA to be carried out and the Board will recommend the SAs to amend their lists accordingly in order to ensure consistency.

When this opinion remains silent on DPIA list entries submitted, it means that the Board is not asking the Swedish Supervisory Authority to take further action.

Finally, the Board recalls that transparency is key for data controllers and data processors. In order to clarify the entries in the list, the Board is of the opinion that making an explicit reference in the lists, for each type of processing, to the criteria set out in the guidelines could improve this transparency. Therefore, the Board considers that an explanation on which

criteria have been taken into account by the Swedish Supervisory Authority to create its list could be added.

2.2 Application of the consistency mechanism to the draft list

The submitted draft list by the Swedish Supervisory Authority relates to the offering of goods or services to data subjects, relates to the monitoring of their behaviour in several Member States and/or may substantially affect the free movement of personal data within the Union mainly because the processing operations in the submitted draft list are not limited to data subjects in this country.

2.3 Analysis of the draft list

Taking into account that:

- a. Article 35 (1) GDPR requires a DPIA when the processing activity is likely to result in a high risk to the rights and freedoms of natural persons; and
- b. Article 35 (3) GDPR provides a non-exhaustive list of types of processing that require a DPIA,

the Board is of the opinion that:

REFERENCE TO THE GUIDELINES

The board is of the opinion that the analysis done in the Working Party 29 Guidelines WP248 are a core element for ensuring consistency across the Union. Thus, it requests the different Supervisor Authorities to add a statement to the document containing their list that clarifies that their list is based on these guidelines and that it complements and further specifies the guidelines.

As the document of the Swedish Supervisory Authority does not contain such a statement, the Board recommends the Swedish Supervisory Authority to amend its document accordingly.

BIOMETRIC DATA

The list submitted by the Swedish Supervisory Authority for an opinion of the Board envisages that the processing of biometric data for the purpose of uniquely identifying a natural person, in conjunction with at least one other criterion, requires a DPIA. On this point, the Board acknowledges that the list aligns with the aim of consistency.

GENETIC DATA

The list submitted by the Swedish Supervisory Authority for an opinion of the Board envisages that the processing of genetic data, in conjunction with at least one other criterion, requires a DPIA. The Board is of the opinion that the processing of genetic data on its own is not necessarily likely to represent a high risk. However, the processing of genetic data in conjunction with at least one other criterion requires a DPIA to be carried out. The Board takes note of the inclusion of this criterion in the list of Swedish Supervisory Authority.

EMPLOYEE MONITORING

The Board is of the opinion that, due to its specific nature, the employee monitoring processing, meeting the criterion of vulnerable data subjects and of systematic monitoring in the guidelines, – could require a DPIA. Given that the list submitted by the Swedish Supervisory Authority for an opinion of the Board already envisages this type of processing as requiring a data protection impact assessment, the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248. In addition, the Board is of the opinion that the WP249 of the Article 29 working party remains valid when defining the concept of the systematic processing of employee data.

PROCESSING USING NEW/INNOVATIVE TECHNOLOGY

The list submitted by the Swedish Supervisory Authority for an opinion of the Board envisages that the processing of personal data using innovative technology in conjunction with at least one other criterion, requires a DPIA. The Board takes note of the inclusion of this criterion in the list.

3. Conclusions / Recommendations

The draft list of the Swedish Supervisory Authority may lead to an inconsistent application of the requirement for a DPIA and the following changes need to made:

- Regarding the reference to the guidelines: the Board requests the Swedish Supervisory Authority to amend its document accordingly.
- Regarding employment monitoring: the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248.

4. Final Remarks

This opinion is addressed to the Datainspektionen (Swedish Supervisory Authority) and will be made public pursuant to Article 64 (5b) GDPR.

According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 21/2018

on the draft list of the competent supervisory authority of Slovakia

regarding

**the processing operations subject to the requirement of a data protection
impact assessment (Article 35.4 GDPR)**

Adopted on 25th September 2018

Contents

1.	Summary of the Facts	4
2.	Assessment	5
2.1	General reasoning of the EDPB regarding the submitted list	5
2.2	Application of the consistency mechanism to the draft list	6
2.3	Analysis of the draft list.....	6
	Indicative nature of the list.....	6
	Reference to the Guidelines	6
	Biometric data.....	6
	Genetic data.....	6
	Biometric 'and' genetic data.....	7
	Location data	7
	Data collected via third parties (article 19 GDPR)	7
	Processing for scientific or historical purposes without consent	7
	Further processing	7
	Exceptions to information to be provided to the data subject according to article 14.5 GDPR	8
	Employee Monitoring	8
	Processing using new/innovative technology	8
3.	Conclusions / Recommendations	8
4.	Final Remarks	9

The European Data Protection Board

Having regard to Article 63, Article 64 (1a), (3) - (8) and Article 35 (1), (3), (4), (6) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (here after GDPR) throughout the European Economic Area. In compliance with article 64.1 GDPR, the Board has to issue an opinion where a supervisory authority intends to adopt a list of processing operations subject to the requirement for a data protection impact assessment pursuant to article 35.4 GDPR. The aim of this opinion is therefore to create a harmonized approach with regard to processing that is cross border or that can affect the free flow of personal data or natural person across the European Union. Even though the GDPR doesn't impose a single list, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by requesting SAs to include some types of processing in their lists, secondly by requesting them to remove some criteria which the Board doesn't consider as necessarily creating high risks for data subjects, and finally by requesting them to use some criteria in a harmonized manner.

(2) With reference to Article 35 (4) and (6) GDPR, the competent supervisory authorities shall establish lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment (hereinafter "DPIA"). They shall, however, apply the consistency mechanism where such lists involve processing operations, which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

(3) While the draft lists of the competent supervisory authorities are subject to the consistency mechanism, this does not mean that the lists should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB assessment/opinion is not to reach a single EU list but rather to avoid significant inconsistencies that may affect the equivalent protection of the data subjects.

(4) The carrying out of a DPIA is only mandatory for the controller pursuant to Article 35 (1) GDPR where processing is "likely to result in a high risk to the rights and freedoms of natural

persons". Article 35 (3) GDPR illustrates what is likely to result in a high risk. This is a non-exhaustive list. The Working Party 29 in the Guidelines on data protection impact assessment¹, as endorsed by the EDPB², has clarified criteria that can help to identify when processing operations are subject to the requirement for a DPIA. The Working Party 29 Guidelines WP248 state that in most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out, however, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

(5) The lists produced by the competent supervisory authorities support the same objective to identify processing operations likely to result in a high risk and processing operations, which therefore require a DPIA. As such, the criteria developed in the Working Party 29 Guidelines should be applied when assessing whether the draft lists of the competent supervisory authorities does not affect the consistent application of the GDPR.

(6) Twenty-two competent supervisory authorities have submitted their draft lists to the EDPB. A global assessment of these draft lists supports the objective of a consistent application of the GDPR even though the complexity of the subject matter increases.

(7) The opinion of the EDPB shall be adopted pursuant to Article 64 (3) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

I. Summary of the Facts

The Úrad na ochranu osobných údajov Slovenskej republiky (hereafter Slovak Supervisory Authority) has submitted its draft list to the EDPB. The decision on the completeness of the file was taken on 11th of July 2018. This period until which the opinion to be adopted has been extended until the 25th of September taking into account the complexity of the subject matter considering that at the same time twenty-two competent supervisory authorities submitted the draft lists and thus the need for a global assessment arose.

¹ WP29, Guidelines on Data Protection Impact Assessment and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP 248 rev. 01).

² EDPB, Endorsement 1/2018.

2. Assessment

2.1 General reasoning of the EDPB regarding the submitted list

Any list submitted to the EDPB has been interpreted as further specifying Art 35.1, which will prevail in any case. Thus, no list can be exhaustive. As the list provided by Slovak Supervisory Authority does not explicitly state this, the Board requests this explanation to be added to the document containing the list.

In compliance with article 35.10 GDPR, the Board is of the opinion that if a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of the legal basis the obligation to carry out a DPIA in accordance with paragraphs 1 to 7 of article 35 GDPR does not apply, unless the Member State deems it necessary.

Further, if the Board requests a DPIA for a certain category of processing and an equivalent measure is already required by national law, the Slovak Supervisory Authority shall add a reference to this measure.

This opinion does not reflect upon items submitted by the Slovak Supervisory Authority, which were deemed outside the scope of Article 35.6 GDPR. This refers to items that neither relate “to the offering of goods or services to data subjects” in several Member States nor to the monitoring of the behaviour of data subjects in several Member States. Additionally, they are not likely to “substantially affect the free movement of personal data within the Union”. This is especially the case for items relating to national legislation and in particular where the obligation to carry out a DPIA is stipulated in national legislation. Further, any processing operations that relate to law enforcement were deemed out of scope, as they are not in scope of the GDPR.

The Board has noted that several supervisory authorities have included in their lists some types of processing which are necessarily local processing. Given that only cross border processing and processing that may affect the free flow of personal data and data subjects are concerned by Article 35.6, the Board will not comment on those local processing.

The opinion aims at defining a consistent core of processing operations that are recurrent in the lists provided by the SAs.

This means that, for a limited number of types of processing operations, that will be defined in a harmonised way, all the Supervisory Authorities will require a DPIA to be carried out and the Board will recommend the SAs to amend their lists accordingly in order to ensure consistency.

When this opinion remains silent on DPIA list entries submitted, it means that the Board is not asking the Slovak Supervisory Authority to take further action.

Finally, the Board recalls that transparency is key for data controllers and data processors. In order to clarify the entries in the list, the Board is of the opinion that making an explicit

reference in the lists, for each type of processing, to the criteria set out in the guidelines could improve this transparency. Therefore, the Board considers that an explanation on which criteria have been taken into account by the Slovak Supervisory Authority to create its list could be added.

2.2 Application of the consistency mechanism to the draft list

The submitted draft list by the Slovak Supervisory Authority relates to the offering of goods or services to data subjects, relates to the monitoring of their behaviour in several Member States and/or may substantially affect the free movement of personal data within the Union mainly because the processing operations in the submitted draft list are not limited to data subjects in this country.

2.3 Analysis of the draft list

Taking into account that:

- a. Article 35 (1) GDPR requires a DPIA when the processing activity is likely to result in a high risk to the rights and freedoms of natural persons; and
- b. Article 35 (3) GDPR provides a non-exhaustive list of types of processing that require a DPIA,

the Board is of the opinion that:

INDICATIVE NATURE OF THE LIST

As the list provided by Slovak Supervisory Authority does not explicitly state that its list is not exhaustive, the Board requests this explanation to be added to the document containing the list.

REFERENCE TO THE GUIDELINES

The board is of the opinion that the analysis done in the Working Party 29 Guidelines WP248 are a core element for ensuring consistency across the Union. Thus, it requests the different Supervisor Authorities to add a statement to the document containing their list that clarifies that their list is based on these guidelines and that it complements and further specifies the guidelines.

As the document of the Slovak Supervisory Authority does not contain such a statement, the Board recommends the Slovak Supervisory Authority to amend its document accordingly.

BIOMETRIC DATA

The list submitted by the Slovak Supervisory Authority for an opinion of the Board envisages that the processing of biometric data for the purpose of uniquely identifying a natural person, or in conjunction with at least one other criterion, requires a DPIA. On this point, the Board acknowledges that the list aligns with the aim of consistency.

GENETIC DATA

The list submitted by the Slovak Supervisory Authority for an opinion of the Board envisages that the processing of genetic data, in conjunction with at least one other criterion, requires

a DPIA. The Board is of the opinion that the processing of genetic data on its own is not necessarily likely to represent a high risk. However, the processing of genetic data in conjunction with at least one other criterion requires a DPIA to be carried out. The Board takes note of the inclusion of this criterion in the list of Slovak Supervisory Authority.

BIOMETRIC 'AND' GENETIC DATA

The list submitted by the Slovak Supervisory Authority for an opinion includes a reference to biometric and genetic data (cumulatively) as a separate entry. The Board has been informed by the Slovak Supervisory Authority that in the original language version biometric and genetic data are in fact considered separately. Therefore, the Board refers to the sections in the opinion on biometric data and genetic data respectively.

LOCATION DATA

The Board is of the opinion that consistency is one of the basic principle of the GDPR. The Board notes that a majority of the lists submitted explicitly contain a reference to the processing of location data. As the list submitted by the Slovak Supervisory Authority for an opinion do not contain such a reference, the Board encourages the Slovak Supervisory Authority to include the processing of location data in its list, together with another criterion.

DATA COLLECTED VIA THIRD PARTIES (ARTICLE 19 GDPR)

The Board is of the opinion that types of processing activities that could deprive the data subjects from their rights in conjunction with at least one other criterion represent a high risk. Further, the Board is of the opinion that a processing activity conducted by the controller under article 19 GDPR and where the information of recipients would prove impossible or require a disproportionate effort only requires a DPIA to be carried out when this processing involves at least one other criterion. The list submitted by the Slovak Supervisory Authority for an opinion of the Board states that this type of processing in conjunction with at least one other criterion falls under the obligation to perform a DPIA. The Board takes note of the inclusion of this criterion in the list.

PROCESSING FOR SCIENTIFIC OR HISTORICAL PURPOSES WITHOUT CONSENT

The Board is of the opinion that the processing of personal data for scientific or historical purposes on its own is not necessarily likely to represent a high risk. However, the processing of personal data for scientific or historical purpose in conjunction with at least one other criterion does require a DPIA to be carried out. The list submitted by the Slovak Supervisory Authority for an opinion of the Board does currently require a DPIA to be carried out when there is a processing of personal data for scientific or historical purpose on its own. The Board requests the Slovak Supervisory Authority to amend its list accordingly, by adding that the item referencing the processing of personal data for scientific or historical purpose requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.

FURTHER PROCESSING

The Board is of the opinion that further processing of personal data should not be a criterion leading to an obligation to do a DPIA, alone or with another criterion. The list submitted by

the Slovak Supervisory Authority for an opinion of the Board does currently require a DPIA to be carried out for the further processing of personal data. The Board requests the Slovak Supervisory Authority to amend its list accordingly, by removing this criterion.

EXCEPTIONS TO INFORMATION TO BE PROVIDED TO THE DATA SUBJECT ACCORDING TO ARTICLE 14.5 GDPR

The Board is of the opinion that types of processing activities that could deprive the data subjects from their rights do not represent a high risk on their own. Therefore, a processing activity conducted by the controller under article 14 GDPR and where the information to be given to the data subjects is subject to an exemption under article 14.5 (b)-(d) could require a DPIA to be carried out only in conjunction with at least one other criterion. The list submitted by the Slovak Supervisory Authority for an opinion of the Board does currently require a DPIA to be done for the processing of data where article 14(5), para (b), (c) and (d) applies on its own. The Board requests the Slovak Supervisory Authority to amend its list accordingly, by adapting the list entry by adding that it requires a DPIA only in conjunction with at least one other criterion.

EMPLOYEE MONITORING

The Board is of the opinion that, due to its specific nature, the employee monitoring processing, meeting the criterion of vulnerable data subjects and of systematic monitoring in the guidelines, – could require a DPIA. Given that the list submitted by the Slovak Supervisory Authority for an opinion of the Board already envisages this type of processing as requiring a data protection impact assessment, the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248. In addition, the Board is of the opinion that the WP249 of the Article 29 working party remains valid when defining the concept of the systematic processing of employee data.

PROCESSING USING NEW/INNOVATIVE TECHNOLOGY

The list submitted by the Slovak Supervisory Authority for an opinion of the Board envisages that the use of new or innovative technology, on its own, requires a DPIA. The Board is of the opinion that the use of innovative technology on its own is not necessarily likely to represent a high risk. However, the use of innovative technology in conjunction with at least one other criterion requires a DPIA to be carried out. Therefore, the Board requests the Slovak Supervisory Authority to amend its list accordingly, firstly by referring in their list to innovative technology and secondly by adding that the item requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.

3. Conclusions / Recommendations

The draft list of the Slovak Supervisory Authority may lead to an inconsistent application of the requirement for a DPIA and the following changes need to made:

- Regarding the indicative nature of the list: the Board requests an explanation to be added to the document containing the list, stating its non-exhaustive nature.

- Regarding the reference to the guidelines: the Board requests the Slovak Supervisory Authority to amend its document accordingly.
- Regarding location data: the Board encourages the Slovak Supervisory Authority to include the processing of location data in its list, together with another criterion.
- Regarding processing of personal data for scientific or historical purposes: the Board requests the Slovak Supervisory Authority to amend its list by adding that the item referencing the processing of personal data for scientific or historical purpose requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.
- Regarding further processing: the Board requests the Slovak Supervisory Authority to amend its list accordingly, by removing this criterion.
- Regarding the exceptions to the information to be given to the data subjects according to article 14.5 GDPR: the Board requests the Slovak Supervisory Authority to amend its list by adding that it requires a DPIA only in conjunction with at least one other criterion.
- Regarding employment monitoring: the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248.
- Regarding processing using new or innovative technology: the Board requests the Slovak Supervisory Authority to amend its list firstly by referring in their list to innovative technology and secondly by adding that the item requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.

4. Final Remarks

This opinion is addressed to the Úrad na ochranu osobných údajov Slovenskej republiky (Slovak Supervisory Authority) and will be made public pursuant to Article 64 (5b) GDPR.

According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 22/2018

on the draft list of the competent supervisory authority of the United Kingdom

regarding

the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)

Adopted on 25th September 2018

Contents

1.	Summary of the Facts	4
2.	Assessment	5
2.1	General reasoning of the EDPB regarding the submitted list	5
2.2	Application of the consistency mechanism to the draft list	6
2.3	Analysis of the draft list.....	6
	Reference to the Guidelines	6
	Biometric data.....	6
	Genetic data.....	6
	Location data	7
	Data collected via third parties (article 19 GDPR)	7
	Exceptions to information to be provided to the data subject according to article 14.5 GDPR	7
	Employee Monitoring	8
	Processing using new/innovative technology	8
3.	Conclusions / Recommendations	8
4.	Final Remarks	9

The European Data Protection Board

Having regard to Article 63, Article 64 (1a), (3) - (8) and Article 35 (1), (3), (4), (6) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (here after GDPR) throughout the European Economic Area. In compliance with article 64.1 GDPR, the Board has to issue an opinion where a supervisory authority intends to adopt a list of processing operations subject to the requirement for a data protection impact assessment pursuant to article 35.4 GDPR. The aim of this opinion is therefore to create a harmonized approach with regard to processing that is cross border or that can affect the free flow of personal data or natural person across the European Union. Even though the GDPR doesn't impose a single list, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by requesting SAs to include some types of processing in their lists, secondly by requesting them to remove some criteria which the Board doesn't consider as necessarily creating high risks for data subjects, and finally by requesting them to use some criteria in a harmonized manner.

(2) With reference to Article 35 (4) and (6) GDPR, the competent supervisory authorities shall establish lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment (hereinafter "DPIA"). They shall, however, apply the consistency mechanism where such lists involve processing operations, which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

(3) While the draft lists of the competent supervisory authorities are subject to the consistency mechanism, this does not mean that the lists should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB assessment/opinion is not to reach a single EU list but rather to avoid significant inconsistencies that may affect the equivalent protection of the data subjects.

(4) The carrying out of a DPIA is only mandatory for the controller pursuant to Article 35 (1) GDPR where processing is "likely to result in a high risk to the rights and freedoms of natural

persons". Article 35 (3) GDPR illustrates what is likely to result in a high risk. This is a non-exhaustive list. The Working Party 29 in the Guidelines on data protection impact assessment¹, as endorsed by the EDPB², has clarified criteria that can help to identify when processing operations are subject to the requirement for a DPIA. The Working Party 29 Guidelines WP248 state that in most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out, however, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

(5) The lists produced by the competent supervisory authorities support the same objective to identify processing operations likely to result in a high risk and processing operations, which therefore require a DPIA. As such, the criteria developed in the Working Party 29 Guidelines should be applied when assessing whether the draft lists of the competent supervisory authorities does not affect the consistent application of the GDPR.

(6) Twenty-two competent supervisory authorities have submitted their draft lists to the EDPB. A global assessment of these draft lists supports the objective of a consistent application of the GDPR even though the complexity of the subject matter increases.

(7) The opinion of the EDPB shall be adopted pursuant to Article 64 (3) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

I. Summary of the Facts

The Information Commissioner's Office (hereafter Supervisory Authority of the United Kingdom) has submitted its draft list to the EDPB. The decision on the completeness of the file was taken on 9th of July 2018. This period until which the opinion to be adopted has been extended until the 25th of September taking into account the complexity of the subject matter considering that at the same time twenty-two competent supervisory authorities submitted the draft lists and thus the need for a global assessment arose.

¹ WP29, Guidelines on Data Protection Impact Assessment and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP 248 rev. 01).

² EDPB, Endorsement 1/2018.

2. Assessment

2.1 General reasoning of the EDPB regarding the submitted list

Any list submitted to the EDPB has been interpreted as further specifying Art 35.1, which will prevail in any case. Thus, no list can be exhaustive.

In compliance with article 35.10 GDPR, the Board is of the opinion that if a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of the legal basis the obligation to carry out a DPIA in accordance with paragraphs 1 to 7 of article 35 GDPR does not apply, unless the Member State deems it necessary.

Further, if the Board requests a DPIA for a certain category of processing and an equivalent measure is already required by national law, the Supervisory Authority of the United Kingdom shall add a reference to this measure.

This opinion does not reflect upon items submitted by the Supervisory Authority of the United Kingdom, which were deemed outside the scope of Article 35.6 GDPR. This refers to items that neither relate “to the offering of goods or services to data subjects” in several Member States nor to the monitoring of the behaviour of data subjects in several Member States. Additionally, they are not likely to “substantially affect the free movement of personal data within the Union”. This is especially the case for items relating to national legislation and in particular where the obligation to carry out a DPIA is stipulated in national legislation. Further, any processing operations that relate to law enforcement were deemed out of scope, as they are not in scope of the GDPR.

The Board has noted that several supervisory authorities have included in their lists some types of processing which are necessarily local processing. Given that only cross border processing and processing that may affect the free flow of personal data and data subjects are concerned by Article 35.6, the Board will not comment on those local processing.

The opinion aims at defining a consistent core of processing operations that are recurrent in the lists provided by the SAs.

This means that, for a limited number of types of processing operations, that will be defined in a harmonised way, all the Supervisory Authorities will require a DPIA to be carried out and the Board will recommend the SAs to amend their lists accordingly in order to ensure consistency.

When this opinion remains silent on DPIA list entries submitted, it means that the Board is not asking the Supervisory Authority of the United Kingdom to take further action.

Finally, the Board recalls that transparency is key for data controllers and data processors. In order to clarify the entries in the list, the Board is of the opinion that making an explicit reference in the lists, for each type of processing, to the criteria set out in the guidelines could improve this transparency. Therefore, the Board considers that an explanation on which

criteria have been taken into account by the Supervisory Authority of the United Kingdom to create its list could be added.

2.2 Application of the consistency mechanism to the draft list

The submitted draft list by the Supervisory Authority of the United Kingdom relates to the offering of goods or services to data subjects, relates to the monitoring of their behaviour in several Member States and/or may substantially affect the free movement of personal data within the Union mainly because the processing operations in the submitted draft list are not limited to data subjects in this country.

2.3 Analysis of the draft list

Taking into account that:

- a. Article 35 (1) GDPR requires a DPIA when the processing activity is likely to result in a high risk to the rights and freedoms of natural persons; and
- b. Article 35 (3) GDPR provides a non-exhaustive list of types of processing that require a DPIA,

the Board is of the opinion that:

REFERENCE TO THE GUIDELINES

The board is of the opinion that the analysis done in the Working Party 29 Guidelines WP248 are a core element for ensuring consistency across the Union. Thus, it requests the different Supervisor Authorities to add a statement to the document containing their list that clarifies that their list is based on these guidelines and that it complements and further specifies the guidelines.

As the document of the Supervisory Authority of the United Kingdom does not contain such a statement, the Board recommends the Supervisory Authority of the United Kingdom to amend its document accordingly.

BIOMETRIC DATA

The list submitted by the Supervisory Authority of the United Kingdom for an opinion of the Board states, that the processing of biometric data falls under the obligation to perform a DPIA on its own. The Board is of the opinion that the processing of biometric data on its own is not necessarily likely to represent a high risk. However, the processing of biometric data for the purpose of uniquely identifying a natural person in conjunction with at least one other criterion requires a DPIA to be carried out. As such, the Board requests the Supervisory Authority of the United Kingdom to amend its list accordingly, by adding that the item referencing the processing of biometric data for the purpose of uniquely identifying a natural person requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion, to be applied without prejudice to article 35(3) GDPR.

GENETIC DATA

The list submitted by the Supervisory Authority of the United Kingdom for an opinion of the Board states, that the processing of genetic data falls under the obligation to perform a DPIA

on its own. The Board is of the opinion that the processing of genetic data on its own is not necessarily likely to represent a high risk. However, the processing of genetic data in conjunction with at least one other criterion requires a DPIA to be carried out. As such, the Board requests the Supervisory Authority of the United Kingdom to amend its list accordingly, by adding that the item referencing the processing of genetic data requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion, to be applied without prejudice to article 35(3) GDPR.

LOCATION DATA

The Board is of the opinion that the processing of location data on its own is not necessarily likely to represent a high risk. However, the processing of location data in conjunction with at least one other criterion requires a DPIA to be carried out. The list submitted by the Supervisory Authority of the United Kingdom for an opinion of the Board does currently require a DPIA to be carried out when there is a processing of location data on its own. The Board requests the Supervisory Authority of the United Kingdom to amend its list accordingly, by adding that the item referencing the processing of location data requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.

DATA COLLECTED VIA THIRD PARTIES (ARTICLE 19 GDPR)

The Board is of the opinion that types of processing activities that could deprive the data subjects from their rights in conjunction with at least one other criterion represent a high risk. Further, the Board is of the opinion that a processing activity conducted by the controller under article 19 GDPR and where the information of recipients would prove impossible or require a disproportionate effort only requires a DPIA to be carried out when this processing involves at least one other criterion. The list submitted by the Supervisory Authority of the United Kingdom for an opinion of the Board states that this type of processing in conjunction with at least one other criterion falls under the obligation to perform a DPIA. The Board takes note of the inclusion of this criterion in the list.

EXCEPTIONS TO INFORMATION TO BE PROVIDED TO THE DATA SUBJECT ACCORDING TO ARTICLE 14.5 GDPR

The Board is of the opinion that types of processing activities that could deprive the data subjects from their rights do not represent a high risk on their own. Therefore, a processing activity conducted by the controller under article 14 GDPR and where the information to be given to the data subjects is subject to an exemption under article 14.5 (b)-(d) could require a DPIA to be carried out only in conjunction with at least one other criterion. The list submitted by the Supervisory Authority of the United Kingdom for an opinion of the Board does currently require a DPIA to be done for the processing of data where article 14(5), para (b), (c) and (d) applies on its own. The Board requests the Supervisory Authority of the United Kingdom to amend its list accordingly, by adding that it requires a DPIA only in conjunction with at least one other criterion.

EMPLOYEE MONITORING

The Board is of the opinion that, due to its specific nature, the employee monitoring processing, meeting the criterion of vulnerable data subjects and of systematic monitoring in the guidelines, – could require a DPIA. Given that the list submitted by the Supervisory Authority of the United Kingdom for an opinion of the Board already envisages this type of processing as requiring a data protection impact assessment, the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248. In addition, the Board is of the opinion that the WP249 of the Article 29 working party remains valid when defining the concept of the systematic processing of employee data.

PROCESSING USING NEW/INNOVATIVE TECHNOLOGY

The list submitted by the Supervisory Authority of the United Kingdom for an opinion of the Board envisages that the use of new or innovative technology, on its own, requires a DPIA. The Board is of the opinion that the use of innovative technology on its own is not necessarily likely to represent a high risk. However, the use of innovative technology in conjunction with at least one other criterion requires a DPIA to be carried out. Therefore, the Board requests the Supervisory Authority of the United Kingdom to amend its list accordingly, firstly by referring in their list to innovative technology and secondly by adding that the item requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.

3. Conclusions / Recommendations

The draft list of the Supervisory Authority of the United Kingdom may lead to an inconsistent application of the requirement for a DPIA and the following changes need to made:

- Regarding the reference to the guidelines: the Board requests the Supervisory Authority of the United Kingdom to amend its document accordingly.
- Regarding biometric data: the Board requests the Supervisory Authority of the United Kingdom to amend its list by adding that the item referencing the processing of biometric data for the purpose of uniquely identifying a natural person requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.
- Regarding genetic data: the Board requests the Supervisory Authority of the United Kingdom to amend its list by adding that the item referencing the processing of genetic data requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.
- Regarding location data: the Board requests the Supervisory Authority of the United Kingdom to amend its list by adding that the item referencing the processing of location data requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.
- Regarding the exceptions to the information to be given to the data subjects according to article 14.5 GDPR: the Board requests the Supervisory Authority of the United Kingdom to amend its list by adding that it requires a DPIA only in conjunction with at least one other criterion.

- Regarding employment monitoring: the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248.
- Regarding processing using new or innovative technology: the Board requests the Supervisory Authority of the United Kingdom to amend its list firstly by referring in their list to innovative technology and secondly by adding that the item requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion.

4. Final Remarks

This opinion is addressed to the Information Commissioner's Office (Supervisory Authority of the United Kingdom) and will be made public pursuant to Article 64 (5b) GDPR.

According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



EDPB Plenary meeting, 04/05.12.2018

Opinion 24/2018 on the draft list of the competent supervisory authority of Denmark regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)

Adopted on 4 December 2018

TABLE OF CONTENTS

1	Summary of the Facts.....	4
2	Assessment.....	5
2.1	General reasoning of the EDPB regarding the submitted list	5
2.2	Application of the consistency mechanism to the draft list	5
2.3	Analysis of the draft list	6
3	Conclusions / Recommendations.....	6
4	Final Remarks	6

Adopted

The European Data Protection Board

Having regard to Article 63, Article 64 (1a), (3) - (8) and Article 35 (1), (3), (4), (6) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (hereafter GDPR) throughout the European Economic Area. In compliance with article 64.1 GDPR, the Board shall issue an opinion where a supervisory authority (SA) intends to adopt a list of processing operations subject to the requirement for a data protection impact assessment pursuant to article 35.4 GDPR. The aim of this opinion is therefore to create a harmonised approach with regard to processing that is cross border or that can affect the free flow of personal data or natural person across the European Union. Even though the GDPR doesn't impose a single list, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by requesting SAs to include some types of processing in their lists, secondly by requesting them to remove some criteria which the Board doesn't consider as necessarily creating high risks for data subjects, and finally by requesting them to use some criteria in a harmonized manner.

(2) With reference to Article 35 (4) and (6) GDPR, the competent supervisory authorities shall establish lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment (hereinafter "DPIA"). They shall, however, apply the consistency mechanism where such lists involve processing operations, which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

(3) While the draft lists of the competent supervisory authorities are subject to the consistency mechanism, this does not mean that the lists should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB assessment/opinion is not to reach a single EU list but rather to avoid significant inconsistencies that may affect the equivalent protection of the data subjects.

(4) The carrying out of a DPIA is only mandatory for the controller pursuant to Article 35 (1) GDPR where processing is "likely to result in a high risk to the rights and freedoms of natural persons". Article 35 (3) GDPR illustrates what is likely to result in a high risk. This is a non-exhaustive list. The

Working Party 29 in the Guidelines on data protection impact assessment¹, as endorsed by the EDPB², has clarified criteria that can help to identify when processing operations are subject to the requirement for a DPIA. The Working Party 29 Guidelines WP248 state that in most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out, however, in some cases a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

(5) The lists produced by the competent supervisory authorities support the same objective to identify processing operations likely to result in a high risk and processing operations, which therefore require a DPIA. As such, the criteria developed in the Working Party 29 Guidelines should be applied when assessing whether the draft lists of the competent supervisory authorities does not affect the consistent application of the GDPR.

(6) Twenty-two competent supervisory authorities received an opinion on their draft lists from the EDPB on 5 September 2018. A further 4 SAs submitted their draft list by early October. A global assessment of these draft lists supports the objective of a consistent application of the GDPR even though the complexity of the subject matter increases.

(7) The opinion of the EDPB shall be adopted pursuant to Article 64 (3) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

1 SUMMARY OF THE FACTS

1. The competent supervisory authority of Denmark has submitted its draft list to the EDPB. The decision on the completeness of the file was taken on the 11th of October 2018.
The period until which the opinion has to be adopted has been extended until the 18th of January 2019 taking into account the complexity of the subject matter considering also the need to factor in the outcome of the review of the twenty-two draft lists previously submitted by competent supervisory authorities and the need for a global assessment of all of them.

¹ WP29, Guidelines on Data Protection Impact Assessment and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 (WP 248 rev. 01).

² EDPB, Endorsement 1/2018.

2 ASSESSMENT

2.1 General reasoning of the EDPB regarding the submitted list

2. Any list submitted to the EDPB has been interpreted as further specifying Art 35.1, which will prevail in any case. Thus, no list can be exhaustive.
3. In compliance with article 35.10 GDPR, the Board is of the opinion that if a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of the legal basis the obligation to carry out a DPIA in accordance with paragraphs 1 to 7 of article 35 GDPR does not apply, unless the Member State deems it necessary.
4. Further, if the Board requests a DPIA for a certain category of processing and an equivalent measure is already required by national law, the Datatilsynet (hereafter Danish Supervisory Authority) shall add a reference to this measure.
5. This opinion does not reflect upon items submitted by the Danish Supervisory Authority, which were deemed outside the scope of Article 35.6 GDPR. This refers to items that neither relate “to the offering of goods or services to data subjects” in several Member States nor to the monitoring of the behaviour of data subjects in several Member States. Additionally, they are not likely to “substantially affect the free movement of personal data within the Union”. This is especially the case for items relating to national legislation and in particular where the obligation to carry out a DPIA is stipulated in national legislation. Further, any processing operations that relate to law enforcement were deemed out of scope, as they are not in scope of the GDPR.
6. The Board has noted that several supervisory authorities have included in their lists some types of processing which are necessarily local processing. Given that only cross border processing and processing that may affect the free flow of personal data and data subjects are concerned by Article 35.6, the Board will not comment on those local processing.
7. The opinion aims at defining a consistent core of processing operations that are recurrent in the lists provided by the SAs.
8. This means that, for a limited number of types of processing operations that will be defined in a harmonized way, all the Supervisory Authorities will require a DPIA to be carried out and the Board will recommend the SAs to amend their lists accordingly in order to ensure consistency.
9. When this opinion remains silent on DPIA list entries submitted, it means that the Board is not asking the Danish Supervisory Authority to take further action.
10. Finally, the Board recalls that transparency is key for data controllers and data processors. In order to clarify the entries in the list, the Board is of the opinion that making an explicit reference in the lists, for each type of processing, to the criteria set out in the guidelines could improve this transparency. Therefore, the Board considers that an explanation on which criteria have been taken into account by the Danish Supervisory Authority to create its list could be added.

2.2 Application of the consistency mechanism to the draft list

11. The draft list submitted by the Danish Supervisory Authority relates to the offering of goods or services to data subjects, relates to the monitoring of their behaviour in several Member States and/or may

substantially affect the free movement of personal data within the Union mainly because the processing operations in the submitted draft list are not limited to data subjects in this country.

2.3 Analysis of the draft list

12. Taking into account that:
 - a. Article 35 (1) GDPR requires a DPIA when the processing activity is likely to result in a high risk to the rights and freedoms of natural persons; and
 - b. Article 35 (3) GDPR provides a non-exhaustive list of types of processing that require a DPIA,

the Board is of the opinion that the draft list of the Danish Supervisory Authority does not contain any dispositions that may lead to an inconsistent application of the requirement for to conduct a DPIA.

3 CONCLUSIONS / RECOMMENDATIONS

13. The draft list of the Danish Supervisory Authority does not contain any dispositions that may lead to an inconsistent application of the requirement for to conduct a DPIA

4 FINAL REMARKS

14. This opinion is addressed to the Datatilsynet (Danish Supervisory Authority) and will be made public pursuant to Article 64 (5b) GDPR.
15. According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Adopted

Opinion of the Board (Art. 64)



EDPB Plenary meeting, 04/05.12.2018

Opinion 25/2018 on the draft list of the competent supervisory authority of Croatia regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)

Adopted on 4 December 2018

TABLE OF CONTENTS

1	Summary of the Facts.....	4
2	Assessment.....	5
2.1	General reasoning of the EDPB regarding the submitted list	5
2.2	Application of the consistency mechanism to the draft list	5
2.3	Analysis of the draft list	6
2.3.1	Reference to the guidelines	6
2.3.2	Biometric data.....	6
2.3.3	Genetic data.....	6
2.3.4	Processing of personal data generated by sensor devices	7
3	Conclusions / Recommendations.....	7
4	Final Remarks	7

Adopted

The European Data Protection Board

Having regard to Article 63, Article 64 (1a), (3) - (8) and Article 35 (1), (3), (4), (6) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (hereafter GDPR) throughout the European Economic Area. In compliance with article 64.1 GDPR, the Board shall issue an opinion where a supervisory authority (SA) intends to adopt a list of processing operations subject to the requirement for a data protection impact assessment pursuant to article 35.4 GDPR. The aim of this opinion is therefore to create a harmonised approach with regard to processing that is cross border or that can affect the free flow of personal data or natural person across the European Union. Even though the GDPR doesn't impose a single list, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by requesting SAs to include some types of processing in their lists, secondly by requesting them to remove some criteria which the Board doesn't consider as necessarily creating high risks for data subjects, and finally by requesting them to use some criteria in a harmonized manner.

(2) With reference to Article 35 (4) and (6) GDPR, the competent supervisory authorities shall establish lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment (hereinafter "DPIA"). They shall, however, apply the consistency mechanism where such lists involve processing operations, which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

(3) While the draft lists of the competent supervisory authorities are subject to the consistency mechanism, this does not mean that the lists should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB assessment/opinion is not to reach a single EU list but rather to avoid significant inconsistencies that may affect the equivalent protection of the data subjects.

(4) The carrying out of a DPIA is only mandatory for the controller pursuant to Article 35 (1) GDPR where processing is "likely to result in a high risk to the rights and freedoms of natural persons". Article 35 (3) GDPR illustrates what is likely to result in a high risk. This is a non-exhaustive list. The

Working Party 29 in the Guidelines on data protection impact assessment¹, as endorsed by the EDPB², has clarified criteria that can help to identify when processing operations are subject to the requirement for a DPIA. The Working Party 29 Guidelines WP248 state that in most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out, however, in some cases a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

(5) The lists produced by the competent supervisory authorities support the same objective to identify processing operations likely to result in a high risk and processing operations, which therefore require a DPIA. As such, the criteria developed in the Working Party 29 Guidelines should be applied when assessing whether the draft lists of the competent supervisory authorities does not affect the consistent application of the GDPR.

(6) Twenty-two competent supervisory authorities received an opinion on their draft lists from the EDPB on 5 September 2018. A further 4 SAs submitted their draft list by early October. A global assessment of these draft lists supports the objective of a consistent application of the GDPR even though the complexity of the subject matter increases.

(7) The opinion of the EDPB shall be adopted pursuant to Article 64 (3) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

1 SUMMARY OF THE FACTS

1. The competent supervisory authority of Croatia has submitted its draft list to the EDPB. The decision on the completeness of the file was taken on the 9th of October 2018.
The period until which the opinion has to be adopted has been extended until the 16th of January 2019 taking into account the complexity of the subject matter considering also the need to factor in the outcome of the review of the twenty-two draft lists previously submitted by competent supervisory authorities and the need for a global assessment of all of them.

¹ WP29, Guidelines on Data Protection Impact Assessment and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 (WP 248 rev. 01).

² EDPB, Endorsement 1/2018.

2 ASSESSMENT

2.1 General reasoning of the EDPB regarding the submitted list

2. Any list submitted to the EDPB has been interpreted as further specifying Art 35.1, which will prevail in any case. Thus, no list can be exhaustive.
3. In compliance with article 35.10 GDPR, the Board is of the opinion that if a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of the legal basis the obligation to carry out a DPIA in accordance with paragraphs 1 to 7 of article 35 GDPR does not apply, unless the Member State deems it necessary.
4. Further, if the Board requests a DPIA for a certain category of processing and an equivalent measure is already required by national law, the Agencija za zaštitu osobnih podataka (hereafter Croatian Supervisory Authority) shall add a reference to this measure.
5. This opinion does not reflect upon items submitted by the Croatian Supervisory Authority, which were deemed outside the scope of Article 35.6 GDPR. This refers to items that neither relate “to the offering of goods or services to data subjects” in several Member States nor to the monitoring of the behaviour of data subjects in several Member States. Additionally, they are not likely to “substantially affect the free movement of personal data within the Union”. This is especially the case for items relating to national legislation and in particular where the obligation to carry out a DPIA is stipulated in national legislation. Further, any processing operations that relate to law enforcement were deemed out of scope, as they are not in scope of the GDPR.
6. The Board has noted that several supervisory authorities have included in their lists some types of processing which are necessarily local processing. Given that only cross border processing and processing that may affect the free flow of personal data and data subjects are concerned by Article 35.6, the Board will not comment on those local processing.
7. The opinion aims at defining a consistent core of processing operations that are recurrent in the lists provided by the SAs.
8. This means that, for a limited number of types of processing operations that will be defined in a harmonized way, all the Supervisory Authorities will require a DPIA to be carried out and the Board will recommend the SAs to amend their lists accordingly in order to ensure consistency.
9. When this opinion remains silent on DPIA list entries submitted, it means that the Board is not asking the Croatian Supervisory Authority to take further action.
10. Finally, the Board recalls that transparency is key for data controllers and data processors. In order to clarify the entries in the list, the Board is of the opinion that making an explicit reference in the lists, for each type of processing, to the criteria set out in the guidelines could improve this transparency. Therefore, the Board considers that an explanation on which criteria have been taken into account by the Croatian Supervisory Authority to create its list could be added.

2.2 Application of the consistency mechanism to the draft list

11. The draft list submitted by the Croatian Supervisory Authority relates to the offering of goods or services to data subjects, relates to the monitoring of their behavior in several Member States and/or

may substantially affect the free movement of personal data within the Union mainly because the processing operations in the submitted draft list are not limited to data subjects in this country.

2.3 Analysis of the draft list

12. Taking into account that:
 - a. Article 35 (1) GDPR requires a DPIA when the processing activity is likely to result in a high risk to the rights and freedoms of natural persons; and
 - b. Article 35 (3) GDPR provides a non-exhaustive list of types of processing that require a DPIA,

the Board is of the opinion that:

2.3.1 Reference to the guidelines

13. The Board is of the opinion that the analysis done in the Working Party 29 Guidelines WP248 are a core element for ensuring consistency across the Union. Thus, it requests the different Supervisory Authorities to add a statement to the document containing their list that clarifies that their list is based on these guidelines and that it complements and further specifies the guidelines.
14. The Croatian Supervisory Authority states: "*The Guidelines on the DPIA have been analyzed as well as available materials and acts of other institutions and authorities in the field of personal data protection in the EU.*" The Board recommends the Croatian Supervisory Authority to clarify in its document that the Working Party 29 Guidelines on Data Protection Impact Assessment (WP 248) are meant, given that not all readers can be assumed to be familiar with them. Further it requests the Croatian Supervisory Authority to clarify that their list is based on these guidelines and that it complements and further specifies the guidelines.

2.3.2 Biometric data

15. The list submitted by the Croatian Supervisory Authority for an opinion of the Board states, that the processing of biometric data in and of itself falls under the obligation to perform a DPIA. The Board is of the opinion that the processing of biometric data is not necessarily likely to represent a high risk per se. However, the processing of biometric data for the purpose of uniquely identifying a natural person in conjunction with at least one other criterion requires a DPIA to be carried out. Therefore the Board requests the Croatian Supervisory Authority to amend its list accordingly, firstly by clarifying that the item referencing the processing of biometric data applies where the purpose of the processing is uniquely identifying a natural person, secondly by adding to this item that only when it is done in conjunction with at least one other criterion a DPIA is required to be carried out, bearing in mind that the DPIA list is to be applied without prejudice to article 35(3) GDPR.

2.3.3 Genetic data

16. The list submitted by the Croatian Supervisory Authority for an opinion of the Board states, that the processing of genetic data in and of itself falls under the obligation to perform a DPIA. The Board is of the opinion that the processing of genetic data is not necessarily likely to represent a high risk per se. However, the processing of genetic data in conjunction with at least one other criterion requires a DPIA to be carried out. Therefore the Board requests the Croatian Supervisory Authority to amend its list accordingly, by adding that the item referencing the processing of genetic data requires a DPIA to

be carried out only when it is done in conjunction of at least one other criterion, to be applied without prejudice to article 35(3) GDPR.

2.3.4 Processing of personal data generated by sensor devices

17. The Board is of the opinion that the processing of personal data generated by sensor devices transmitting data over the Internet or other information transfer technologies should not be a criterion leading to an obligation to do a DPIA, alone or with another criterion, is not necessarily likely to represent a high risk, as the current wording of this item of the draft DPIA list is overly broad in scope. Given that the list submitted by the Croatian Supervisory Authority for an opinion of the Board envisages this type of processing as requiring a data protection impact assessment, the Board requests the Croatian Supervisory Authority to remove this item from its list.

3 CONCLUSIONS / RECOMMENDATIONS

18. The draft list of the Croatian Supervisory Authority may lead to an inconsistent application of the requirement for a DPIA and the following changes need to made:
- Regarding the reference to the guidelines: the Board requests the Croatian Supervisory Authority to clarify that their list is based on these guidelines and that it complements and further specifies the guidelines.
 - Regarding biometric data: the Board requests the Croatian Supervisory Authority to amend its list firstly by clarifying that the item referencing the processing of biometric data applies where the purpose of the processing is uniquely identifying a natural person, secondly by adding to this item that only when it is done in conjunction with at least one other criterion a DPIA is required to be carried out.
 - Regarding genetic data: the Board requests the Croatian Supervisory Authority to amend its list by adding that the item referencing the processing of genetic data requires a DPIA to be carried out only when it is done in conjunction with at least one other criterion.
 - Regarding processing of personal data generated by sensor devices the Board requests the Croatian Supervisory Authority to remove this item from its list.

4 FINAL REMARKS

19. This opinion is addressed to the Agencija za zaštitu osobnih podataka (Croatian Supervisory Authority) and will be made public pursuant to Article 64 (5b) GDPR.
20. According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

For the European Data Protection Board

The Chair

Adopted

(Andrea Jelinek)

Adopted

8

Opinion of the Board (Art. 64)



EDPB Plenary meeting, 04/05.12.2018

Opinion 26/2018 on the draft list of the competent supervisory authority of Luxembourg regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)

Adopted on 4 December 2018

TABLE OF CONTENTS

1	Summary of the Facts.....	4
2	Assessment.....	5
2.1	General reasoning of the EDPB regarding the submitted list	5
2.2	Application of the consistency mechanism to the draft list	5
2.3	Analysis of the draft list	6
2.3.1	Biometric data.....	6
2.3.2	Genetic data.....	6
2.3.3	Systematic monitoring of publicly accessible areas.....	6
2.3.4	Indirect collection of personal data when it is not possible / feasible to guarantee the right of information (article 14.5 GDPR)	7
3	Conclusions / Recommendations.....	7
4	Final Remarks	8

The European Data Protection Board

Having regard to Article 63, Article 64 (1a), (3) - (8) and Article 35 (1), (3), (4), (6) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (hereafter GDPR) throughout the European Economic Area. In compliance with article 64.1 GDPR, the Board shall issue an opinion where a supervisory authority (SA) intends to adopt a list of processing operations subject to the requirement for a data protection impact assessment pursuant to article 35.4 GDPR. The aim of this opinion is therefore to create a harmonised approach with regard to processing that is cross border or that can affect the free flow of personal data or natural person across the European Union. Even though the GDPR doesn't impose a single list, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by requesting SAs to include some types of processing in their lists, secondly by requesting them to remove some criteria which the Board doesn't consider as necessarily creating high risks for data subjects, and finally by requesting them to use some criteria in a harmonized manner.

(2) With reference to Article 35 (4) and (6) GDPR, the competent supervisory authorities shall establish lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment (hereinafter "DPIA"). They shall, however, apply the consistency mechanism where such lists involve processing operations, which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

(3) While the draft lists of the competent supervisory authorities are subject to the consistency mechanism, this does not mean that the lists should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB assessment/opinion is not to reach a single EU list but rather to avoid significant inconsistencies that may affect the equivalent protection of the data subjects.

(4) The carrying out of a DPIA is only mandatory for the controller pursuant to Article 35 (1) GDPR where processing is "likely to result in a high risk to the rights and freedoms of natural persons". Article 35 (3) GDPR illustrates what is likely to result in a high risk. This is a non-exhaustive list. The

Working Party 29 in the Guidelines on data protection impact assessment¹, as endorsed by the EDPB², has clarified criteria that can help to identify when processing operations are subject to the requirement for a DPIA. The Working Party 29 Guidelines WP248 state that in most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out, however, in some cases a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

(5) The lists produced by the competent supervisory authorities support the same objective to identify processing operations likely to result in a high risk and processing operations, which therefore require a DPIA. As such, the criteria developed in the Working Party 29 Guidelines should be applied when assessing whether the draft lists of the competent supervisory authorities does not affect the consistent application of the GDPR.

(6) Twenty-two competent supervisory authorities received an opinion on their draft lists from the EDPB on 5 September 2018. A further 4 SAs submitted their draft list by early October. A global assessment of these draft lists supports the objective of a consistent application of the GDPR even though the complexity of the subject matter increases.

(7) The opinion of the EDPB shall be adopted pursuant to Article 64 (3) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

1 SUMMARY OF THE FACTS

1. The competent supervisory authority of Luxembourg has submitted its draft list to the EDPB. The decision on the completeness of the file was taken on the 28th of July 2018. The period until which the opinion has to be adopted has been extended until the 5th of December 2018 taking into account the complexity of the subject matter considering also the need to factor in the outcome of the review of the twenty-two draft lists previously submitted by competent supervisory authorities and the need for a global assessment of all of them.

¹ WP29, Guidelines on Data Protection Impact Assessment and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 (WP 248 rev. 01).

² EDPB, Endorsement 1/2018.

2 ASSESSMENT

2.1 General reasoning of the EDPB regarding the submitted list

2. Any list submitted to the EDPB has been interpreted as further specifying Art 35.1, which will prevail in any case. Thus, no list can be exhaustive.
3. In compliance with article 35.10 GDPR, the Board is of the opinion that if a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of the legal basis the obligation to carry out a DPIA in accordance with paragraphs 1 to 7 of article 35 GDPR does not apply, unless the Member State deems it necessary.
4. Further, if the Board requests a DPIA for a certain category of processing and an equivalent measure is already required by national law, the Commission nationale pour la protection des données (hereafter Luxembourg Supervisory Authority) shall add a reference to this measure.
5. This opinion does not reflect upon items submitted by the Luxembourg Supervisory Authority, which were deemed outside the scope of Article 35.6 GDPR. This refers to items that neither relate “to the offering of goods or services to data subjects” in several Member States nor to the monitoring of the behaviour of data subjects in several Member States. Additionally, they are not likely to “substantially affect the free movement of personal data within the Union”. This is especially the case for items relating to national legislation and in particular where the obligation to carry out a DPIA is stipulated in national legislation. Further, any processing operations that relate to law enforcement were deemed out of scope, as they are not in scope of the GDPR.
6. The Board has noted that several supervisory authorities have included in their lists some types of processing which are necessarily local processing. Given that only cross border processing and processing that may affect the free flow of personal data and data subjects are concerned by Article 35.6, the Board will not comment on those local processing.
7. The opinion aims at defining a consistent core of processing operations that are recurrent in the lists provided by the SAs.
8. This means that, for a limited number of types of processing operations that will be defined in a harmonized way, all the Supervisory Authorities will require a DPIA to be carried out and the Board will recommend the SAs to amend their lists accordingly in order to ensure consistency.
9. When this opinion remains silent on DPIA list entries submitted, it means that the Board is not asking the Luxembourg Supervisory Authority to take further action.
10. Finally, the Board recalls that transparency is key for data controllers and data processors. In order to clarify the entries in the list, the Board is of the opinion that making an explicit reference in the lists, for each type of processing, to the criteria set out in the guidelines could improve this transparency. Therefore, the Board considers that an explanation on which criteria have been taken into account by the Luxembourg Supervisory Authority to create its list could be added.

2.2 Application of the consistency mechanism to the draft list

11. The draft list submitted by the Luxembourg Supervisory Authority relates to the offering of goods or services to data subjects, relates to the monitoring of their behavior in several Member States and/or

may substantially affect the free movement of personal data within the Union mainly because the processing operations in the submitted draft list are not limited to data subjects in this country.

2.3 Analysis of the draft list

12. Taking into account that:
- Article 35 (1) GDPR requires a DPIA when the processing activity is likely to result in a high risk to the rights and freedoms of natural persons; and
 - Article 35 (3) GDPR provides a non-exhaustive list of types of processing that require a DPIA,

the Board is of the opinion that:

2.3.1 Biometric data

13. The list submitted by the Luxembourg Supervisory Authority for an opinion of the Board states, that the processing of biometric data as defined under GDPR article 4(14) and which has as a purpose identification of data subjects in and of itself falls under the obligation to perform a DPIA. The Board is of the opinion that the processing of biometric data is not necessarily likely to represent a high risk per se. However, the processing of biometric data for the purpose of uniquely identifying a natural person in conjunction with at least one other criterion requires a DPIA to be carried out. Therefore the Board requests the Luxembourg Supervisory Authority to amend its list accordingly, by adding that the item referencing the processing of biometric data for the purpose of uniquely identifying a natural person requires a DPIA to be carried out only when it is done in conjunction with at least one other criterion, to be applied without prejudice to article 35(3) GDPR.

2.3.2 Genetic data

14. The list submitted by the Luxembourg Supervisory Authority for an opinion of the Board states, that the processing of genetic data in and of itself falls under the obligation to perform a DPIA. The Board is of the opinion that the processing of genetic data is not necessarily likely to represent a high risk per se. However, the processing of genetic data in conjunction with at least one other criterion requires a DPIA to be carried out. Therefore the Board requests the Luxembourg Supervisory Authority to amend its list accordingly, by adding that the item referencing the processing of genetic data requires a DPIA to be carried out only when it is done in conjunction with at least one other criterion, to be applied without prejudice to article 35(3) GDPR.

2.3.3 Systematic monitoring of publicly accessible areas

15. The list submitted by the Luxembourg Supervisory Authority for an opinion of the Board states, that the processing activities that consist of or include regular and systematic monitoring of publicly accessible areas falls under the obligation to perform a DPIA – provided that data is stored. The Board is of the opinion that the processing activities that consist of or include regular and systematic monitoring of publicly accessible areas are not necessarily likely to represent a high risk. However, in conjunction with at least one other criterion such processing is likely to present a high risk and requires a DPIA to be carried out. Therefore the Board requests the Luxembourg Supervisory Authority to amend its list accordingly, by adding that the item referencing the processing activities that consist of or include regular and systematic monitoring of publicly accessible areas requires a DPIA to be carried

out only when it is done in conjunction with at least one other criterion, to be applied without prejudice to article 35(3) GDPR.

2.3.4 Indirect collection of personal data when it is not possible / feasible to guarantee the right of information (article 14.5 GDPR)

16. The list submitted by the Luxembourg Supervisory Authority for an opinion of the Board states, that the processing activities based on indirect collection of personal data when it is not possible / feasible to guarantee the right of information fall under the obligation to perform a DPIA. The Board is of the opinion that types of processing activities that could deprive the data subjects from their rights do not necessarily represent a high risk on their own. Therefore, a processing activity conducted by the controller under article 14 GDPR and where the information to be given to the data subjects is subject to an exemption under article 14.5 could require a DPIA to be carried out only in conjunction with at least one other criterion. The Board points out that the exceptions to the obligation of informing the data subjects are only possible when the data has been collected by a third party. Therefore in this case the mention of indirect collection does not count as a second criterion.
17. The Board requests the Luxembourg Supervisory Authority to amend its list accordingly, by adding that the item referencing the processing activities based on indirect collection of personal data when it is not possible / feasible to guarantee the right of information requires a DPIA to be carried out only when it is done in conjunction with at least one other criterion.

3 CONCLUSIONS / RECOMMENDATIONS

18. The draft list of the Luxembourg Supervisory Authority may lead to an inconsistent application of the requirement for a DPIA and the following changes need to made:
 - Regarding biometric data: the Board requests the Luxembourg Supervisory Authority to amend its list by adding that the item referencing the processing of biometric data for the purpose of uniquely identifying a natural person requires a DPIA to be carried out only when it is done in conjunction with at least one other criterion
 - Regarding genetic data: the Board requests the Luxembourg Supervisory Authority to amend its list by adding that the item referencing the processing of genetic data requires a DPIA to be carried out only when it is done in conjunction with at least one other criterion.
 - Regarding the systematic monitoring of publicly available areas: the Board requests the Luxembourg Supervisory Authority to amend its list by adding that the item referencing the processing activities that consist of or include regular and systematic monitoring of publicly accessible areas requires a DPIA to be carried out only when it is done in conjunction with at least one other criterion
 - Regarding the Indirect collection of personal data when it is not possible / feasible to guarantee the right of information: the Board requests the Luxembourg Supervisory Authority to amend its list by adding that the item referencing the processing activities based on indirect collection of personal data when it is not possible / feasible to guarantee the right of information requires a DPIA to be carried out only when it is done in conjunction with at least one other criterion.

4 FINAL REMARKS

19. This opinion is addressed to the Commission nationale pour la protection des données (Luxembourg Supervisory Authority) and will be made public pursuant to Article 64 (5b) GDPR.
20. According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Adopted

Opinion of the Board (Art. 64)



EDPB Plenary meeting, 04/05.12.2018

Opinion 27/2018 on the draft list of the competent supervisory authority of Slovenia regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)

Adopted on 4 December 2018

TABLE OF CONTENTS

1	Summary of the Facts.....	4
2	Assessment.....	5
2.1	General reasoning of the EDPB regarding the submitted list	5
2.2	Application of the consistency mechanism to the draft list	5
2.3	Analysis of the draft list	6
2.3.1	Biometric data.....	6
2.3.2	Genetic data.....	6
2.3.3	Processing posing a significant risk	6
2.3.4	Processing posing a high risk	6
3	Conclusions / Recommendations.....	7
4	Final Remarks	7

Adopted

The European Data Protection Board

Having regard to Article 63, Article 64 (1a), (3) - (8) and Article 35 (1), (3), (4), (6) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (hereafter GDPR) throughout the European Economic Area. In compliance with article 64.1 GDPR, the Board shall issue an opinion where a supervisory authority (SA) intends to adopt a list of processing operations subject to the requirement for a data protection impact assessment pursuant to article 35.4 GDPR. The aim of this opinion is therefore to create a harmonised approach with regard to processing that is cross border or that can affect the free flow of personal data or natural person across the European Union. Even though the GDPR doesn't impose a single list, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by requesting SAs to include some types of processing in their lists, secondly by requesting them to remove some criteria which the Board doesn't consider as necessarily creating high risks for data subjects, and finally by requesting them to use some criteria in a harmonized manner.

(2) With reference to Article 35 (4) and (6) GDPR, the competent supervisory authorities shall establish lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment (hereinafter "DPIA"). They shall, however, apply the consistency mechanism where such lists involve processing operations, which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

(3) While the draft lists of the competent supervisory authorities are subject to the consistency mechanism, this does not mean that the lists should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB assessment/opinion is not to reach a single EU list but rather to avoid significant inconsistencies that may affect the equivalent protection of the data subjects.

(4) The carrying out of a DPIA is only mandatory for the controller pursuant to Article 35 (1) GDPR where processing is "likely to result in a high risk to the rights and freedoms of natural persons". Article 35 (3) GDPR illustrates what is likely to result in a high risk. This is a non-exhaustive list. The

Working Party 29 in the Guidelines on data protection impact assessment¹, as endorsed by the EDPB², has clarified criteria that can help to identify when processing operations are subject to the requirement for a DPIA. The Working Party 29 Guidelines WP248 state that in most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out, however, in some cases a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

(5) The lists produced by the competent supervisory authorities support the same objective to identify processing operations likely to result in a high risk and processing operations, which therefore require a DPIA. As such, the criteria developed in the Working Party 29 Guidelines should be applied when assessing whether the draft lists of the competent supervisory authorities does not affect the consistent application of the GDPR.

(6) Twenty-two competent supervisory authorities received an opinion on their draft lists from the EDPB on 5 September 2018. A further 4 SAs submitted their draft list by early October. A global assessment of these draft lists supports the objective of a consistent application of the GDPR even though the complexity of the subject matter increases.

(7) The opinion of the EDPB shall be adopted pursuant to Article 64 (3) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

1 SUMMARY OF THE FACTS

1. The competent supervisory authority of Slovenia has submitted its draft list to the EDPB. The decision on the completeness of the file was taken on the 9th of October 2018.
The period until which the opinion has to be adopted has been extended until the 16th of January 2019 taking into account the complexity of the subject matter considering also the need to factor in the outcome of the review of the twenty-two draft lists previously submitted by competent supervisory authorities and the need for a global assessment of all of them.

¹ WP29, Guidelines on Data Protection Impact Assessment and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 (WP 248 rev. 01).

² EDPB, Endorsement 1/2018.

2 ASSESSMENT

2.1 General reasoning of the EDPB regarding the submitted list

2. Any list submitted to the EDPB has been interpreted as further specifying Art 35.1, which will prevail in any case. Thus, no list can be exhaustive.
3. In compliance with article 35.10 GDPR, the Board is of the opinion that if a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of the legal basis the obligation to carry out a DPIA in accordance with paragraphs 1 to 7 of article 35 GDPR does not apply, unless the Member State deems it necessary.
4. Further, if the Board requests a DPIA for a certain category of processing and an equivalent measure is already required by national law, the Informacijski pooblaščenec (hereafter Slovenian Supervisory Authority) shall add a reference to this measure.
5. This opinion does not reflect upon items submitted by the Slovenian Supervisory Authority, which were deemed outside the scope of Article 35.6 GDPR. This refers to items that neither relate “to the offering of goods or services to data subjects” in several Member States nor to the monitoring of the behaviour of data subjects in several Member States. Additionally, they are not likely to “substantially affect the free movement of personal data within the Union”. This is especially the case for items relating to national legislation and in particular where the obligation to carry out a DPIA is stipulated in national legislation. Further, any processing operations that relate to law enforcement were deemed out of scope, as they are not in scope of the GDPR.
6. The Board has noted that several supervisory authorities have included in their lists some types of processing which are necessarily local processing. Given that only cross border processing and processing that may affect the free flow of personal data and data subjects are concerned by Article 35.6, the Board will not comment on those local processing.
7. The opinion aims at defining a consistent core of processing operations that are recurrent in the lists provided by the SAs.
8. This means that, for a limited number of types of processing operations that will be defined in a harmonized way, all the Supervisory Authorities will require a DPIA to be carried out and the Board will recommend the SAs to amend their lists accordingly in order to ensure consistency.
9. When this opinion remains silent on DPIA list entries submitted, it means that the Board is not asking the Slovenian Supervisory Authority to take further action.
10. Finally, the Board recalls that transparency is key for data controllers and data processors. In order to clarify the entries in the list, the Board is of the opinion that making an explicit reference in the lists, for each type of processing, to the criteria set out in the guidelines could improve this transparency. Therefore, the Board considers that an explanation on which criteria have been taken into account by the Slovenian Supervisory Authority to create its list could be added.

2.2 Application of the consistency mechanism to the draft list

11. The draft list submitted by the Slovenian Supervisory Authority relates to the offering of goods or services to data subjects, relates to the monitoring of their behavior in several Member States and/or

may substantially affect the free movement of personal data within the Union mainly because the processing operations in the submitted draft list are not limited to data subjects in this country.

2.3 Analysis of the draft list

12. Taking into account that:
 - a. Article 35 (1) GDPR requires a DPIA when the processing activity is likely to result in a high risk to the rights and freedoms of natural persons; and
 - b. Article 35 (3) GDPR provides a non-exhaustive list of types of processing that require a DPIA,

the Board is of the opinion that:

2.3.1 Biometric data

13. The Board is of the opinion that the processing of biometric data for the purpose of uniquely identifying a natural person in conjunction with at least one other criterion requires a DPIA to be carried out. The list submitted by the Slovenian Supervisory Authority incorporates this requirement implicitly, given that the list deems a DPIA necessary when the processing of sensitive data occurs in conjunction with another criterion from the list.
14. The Board recommends mentioning explicitly biometric data which is processed for the purpose of uniquely identifying a natural person in the DPIA list as a criterion which, as indicated in the introduction of the submitted DPIA list, when occurring together with another criterion from the list leads to a DPIA being compulsory.

2.3.2 Genetic data

15. The Board is of the opinion that the processing of genetic data in conjunction with at least one other criterion requires a DPIA to be carried out. The list submitted by the Slovenian Supervisory Authority incorporates this requirement implicitly, given that the list deems a DPIA necessary when the processing of sensitive data occurs in conjunction with another criterion from the list.
16. The Board recommends mentioning explicitly genetic data in the DPIA list as a criterion which, as indicated in the introduction of the submitted DPIA list, when occurring together with another criterion from the list leads to a DPIA being compulsory.

2.3.3 Processing posing a significant risk

17. The Board is of the opinion that the notion “may pose a significant risk”, as used under item 4 ‘Processing of special categories of personal data’ of the list submitted by the Slovenian Supervisory Authority, may lead to confusion as to whether the level of risk is equivalent to the term “likely to result in a high risk” as stated by article 35.1 GDPR. Therefore, the Board requests the Slovenian Supervisory Authority to remove the reference to significant risk.

2.3.4 Processing posing a high risk

18. The list submitted by the Slovenian Supervisory Authority mentions, under item 4 ‘Processing of special categories of personal data’, that a DPIA is required “when processing of special categories of personal data, data on criminal or minor offences represent a high-risk for the rights of the individual”. The mention of “high risk” here should be taken as a reference to the term “likely to result in a high

risk” as stated by article 35.1 GDPR and not as a separate condition. The Board requests the Slovenian Supervisory Authority to remove the repetition of “high risk” from this item of its list.

3 CONCLUSIONS / RECOMMENDATIONS

19. The draft list of the Slovenian Supervisory Authority may lead to an inconsistent application of the requirement for a DPIA and the following changes need to made:

- Regarding biometric data: the Board requests the Slovenian Supervisory Authority to amend its list by mentioning explicitly the processing of biometric data which is processed for the purpose of uniquely identifying a natural person in conjunction with at least one other criterion;
- Regarding genetic data: the Board requests the Slovenian Supervisory Authority to amend its list by mentioning explicitly the processing of genetic data in conjunction with at least one other criterion in the DPIA list;
- Regarding processing posing a significant risk: the Board requests the Slovenian Supervisory Authority to amend its list by removing the reference to “significant risk”
- Regarding processing posing a high risk: the Board requests the Slovenian Supervisory Authority to amend its list by removing the reference to “high risk”

4 FINAL REMARKS

20. This opinion is addressed to the Informacijski pooblaščenec (Slovenian Supervisory Authority) and will be made public pursuant to Article 64 (5b) GDPR.

21. According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Adopted

Opinion of the Board (Art. 70.1.s)



Opinion 28/2018
**regarding the European Commission Draft Implementing
Decision**
on the adequate protection of personal data in Japan

Adopted on 5 December 2018

Table of contents

1	EXECUTIVE SUMMARY.....	4
1.1	Areas of convergence.....	5
1.2	General challenges	5
1.3	Specific commercial aspects.....	6
1.3.1	Concerns of the EDPB with regards to key data protection principles	6
1.3.2	Need for clarification.....	7
1.4	On the access by public authorities to data transferred to Japan	7
1.5	Conclusion	7
2	INTRODUCTION	8
2.1	Japan's data protection framework	8
2.2	Scope of the EDPB's assessment.....	9
2.3	General comments and concerns.....	10
2.3.1	Specificities of this type of adequacy decision.....	10
2.3.2	Certainty of translations.....	10
2.3.3	Sectorial Adequacy	11
2.3.4	Binding nature of Supplementary Rules and of PPC Guidelines	11
2.3.5	Periodic review of the adequacy finding.....	12
2.3.6	International commitments entered into by Japan	12
2.3.7	Powers of DPAs to bring actions concerning the validity of an adequacy decision before a court.....	13
3	COMMERCIAL ASPECTS	13
3.1	Content principles	13
3.1.1	Concepts	13
3.1.2	Grounds for lawful and fair processing for legitimate purposes.....	16
3.1.3	The transparency principle.....	17
3.1.4	Restrictions on onward transfers	18
3.1.5	Direct marketing.....	21
3.1.6	Automated decision making and profiling	21
3.2	Procedural and enforcement mechanisms	22
3.2.1	Competent independent Supervisory Authority	22
3.2.2	The data protection system must ensure a good level of compliance	22
3.2.3	The data protection system must provide support and help to individual data subjects in the exercise of their rights and appropriate redress mechanisms	23
4	ON THE ACCESS BY PUBLIC AUTHORITIES TO THE DATA TRANSFERRED TO JAPAN	24

4.1	Law enforcement access to data.....	25
4.1.1	Procedures for accessing data in the field of criminal law.....	25
4.1.2	Oversight in the field of criminal law	27
4.1.3	Redress in the field of criminal law	30
4.2	Access for national security purposes.....	36
4.2.1	Scope of surveillance.....	36
4.2.2	Voluntary disclosure in case of national security.....	38
4.2.3	Oversight	38
4.2.4	Redress mechanism.....	40

The European Data Protection Board

Having regard to Article 70.1(s) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 12 and Article 22 of its Rules of Procedure of 25 May 2018,

HAS ADOPTED THE FOLLOWING OPINION:

1 EXECUTIVE SUMMARY

1. The European Commission endorsed its draft implementing decision on the adequate protection of personal data by Japan pursuant to the General Data Protection Regulation (hereinafter: GDPR)¹ on 5 September 2018². Following this, the European Commission initiated the procedure for its formal adoption.
2. On 25 September 2018, the European Commission asked for the opinion of the European Data Protection Board (“EDPB”)³. The Commission was requested to provide the EDPB with all the necessary documentation with regards to this country, including any relevant correspondence with the government of Japan.
3. In the light of the discussions held with the EDPB, the European Commission modified twice its draft adequacy decision, and sent its last version on 13 November 2018⁴. The EDPB has based its present Opinion on this latest version of the draft implementing decision (hereinafter “draft adequacy decision”).
4. The EDPB’s assessment of the level of protection ensured by the Commission’s adequacy decision has been made on the examination of the decision itself as well as on the basis of an analysis of the documentation made available⁵—by the Commission⁶.
5. The EDPB focused on the assessment of both the commercial aspects of the draft adequacy decision and on the government access to personal data transferred from the EU for the purposes of law enforcement and national security, including the legal remedies available to EU individuals. The EDPB

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

² See Press release http://europa.eu/rapid/press-release_IP-18-5433_en.htm.

³ Pursuant to Article 70 (1) (s) of the GDPR.

⁴ See Annex I of the EDPB Opinion for the updated version of the draft European Commission implementing decision.

⁵ The EDPB based its analysis on translations provided by the Japanese authorities verified by the European Commission

⁶ See Annex II of the EDPB Opinion for the list of documents not provided by the European Commission to the EDPB.

also assessed whether the safeguards provided under the Japanese legal framework are in place and effective.

6. The EDPB has used as a main reference for this work its adequacy referential⁷ adopted in February 2018.

1.1 Areas of convergence

7. The EDPB's key objective has been to give an opinion to the European Commission on the level of protection afforded to individuals in the Japanese framework. It is important to recognise that the EDPB does not expect the Japanese legal framework to replicate European data protection law.
8. However, the EDPB recalls that to be considered providing an adequate level of protection, the case law of the CJEU as well as Article 45 of the GDPR require that the third country's legislation needs to be aligned to the essence of the fundamental principles enshrined in the GDPR. In the areas of data protection, the EDPB further notes that there are key areas of alignment between the GDPR framework and the Japanese framework on certain core provisions such as data accuracy and minimisation, storage limitation, data security, purpose limitation and an independent supervisory authority, the Personal Information Protection Commission (PPC).
9. In addition to the above, the EDPB welcomes the efforts made by the European Commission and the Japanese authorities to ensure that Japan provides an adequate level of protection to that of the GDPR especially by filling the gaps between the GDPR and the Japanese data protection framework through the adoption of additional rules by the PPC applicable only to personal data transferred from the EU to Japan, the Supplementary Rules. For example, the EDPB notes that the PPC agreed to treat further categories of data as sensitive data (sensitive data under the Japanese legislation do not include sex orientation nor trade union membership). In addition, the Supplementary Rules ensure that data subject rights will apply to all personal data transferred from the EU, irrespective of their retention period (whereas the Japanese legal system provides that data subject rights do not apply to personal data that are set to be deleted within a period of six months).
10. The EDPB also notes the efforts of the European Commission in strengthening the adequacy decision in response to the concerns raised by the EDPB.

1.2 General challenges

11. Nonetheless, challenges remain and the EDPB suggests the following as the main areas that should be strengthened and closely monitored in the Japanese system.
12. The first challenge relates to the monitoring of this new architecture of adequacy, which is combining an existing legal framework with specific Supplementary Rules, to ensure that it will be a sustainable and reliable system that will not raise **practical issues regarding the concrete and efficient compliance** by Japanese entities and enforcement by the PPC.
13. Secondly, the EDPB takes note of the repeated commitments and reassurances of the European Commission and of the Japanese authorities regarding the binding and enforceable nature of the Supplementary Rules whilst inviting the European Commission to **continuously monitor their binding nature and effective application in Japan** as their legal value is an absolutely essential element of the EU – Japan adequacy. With respect to the PPC guidelines, the EDPB would welcome clarifications in

⁷ WP254, Adequacy Referential, 6 February 2018.

the draft adequacy decision in relation to **their binding nature and asks the Commission to attentively monitor this aspect⁸**.

[1.3 Specific commercial aspects](#)

14. In the area of the commercial aspects of the draft EU – Japan adequacy decision, the EDPB has some specific concerns and would like to request clarifications on some important matters.
 - 14.1 [Concerns of the EDPB with regards to key data protection principles](#)
15. The EDPB welcomes that the Supplementary Rules exclude that personal data transferred from the EU is further transferred to a third country on the basis of APEC – CBPRs. In addition, the EDPB recognises that in its new draft of the adequacy decision, the European Commission committed itself to suspend the adequacy decision when onward transfers no longer ensure the continuity of protection.
16. Under the Japanese legislation, one of the legal basis for onward transfers is the recognition of a third country as providing an adequate level of protection to that of Japan. However, the assessment of a third country as adequate by Japan seems not to include the specific “Supplementary Rules” negotiated between the European Commission and the PPC which are only applicable to EU personal data in order to provide for a level of protection essentially equivalent to the GDPR standards. It follows that EU personal data that are transferred from Japan to another third country not recognised as having an essentially equivalent data protection framework to the GDPR on the basis of a Japanese adequacy will not necessarily enjoy the specific protection for EU personal data anymore.
17. **It should however be borne in mind that onward transfers of personal data may occur to third countries which become subject to a possible later Japanese adequacy decision. These third countries may not have been subject of a previous assessment or adequacy finding of the EU. At this point the COM should take over its monitoring role and ensure the level of protection of EU data is maintained or consider suspension of this adequacy decision.**
18. Moreover, the EDPB has concerns in relation to the **consent and transparency obligations** of data controllers (PIHBOs). The EDPB made a careful check of these elements for the reason that, differently to European data protection law, the use of consent as a basis for processing and for transfers has a central role in the Japanese legal system. For example, the EDPB has concerns regarding the notion of consent which is not defined in a way to include the right to withdrawal, an essential element under EU law to ensure the data subject's genuine control over his/her personal data. Regarding the transparency obligations of a PIHBO, there are doubts as to whether proactive information is given to data subjects.
19. The EDPB is concerned that the **Japanese redress system** may not be of easy access to individuals in the EU needing support or wishing to make a complaint in light of the fact that PPC's support is available via Helpline and in Japanese only. The same issue exists with the mediation service provided by the PPC as the system is not publicised on the English version of the PPC's website whilst important informative documents, such as the frequently asked questions on the APPI, are also available in Japanese only. In this respect, the EDPB would welcome if the Commission could discuss with the PPC the possibility of setting up an online service, at least in English, aimed at providing support to, and handle complaints of, individuals in the EU – similar to the one envisaged in Annex II of this adequacy decision. The European Commission will also need to monitor closely the effectiveness of sanctions and of relevant remedies.

⁸ See Section 1.3.4 of the present opinion for more information.

1.3.2 Need for clarification

20. The EDPB would welcome assurances on some aspects of the draft adequacy decision on which further clarification is still needed.
21. These relate for example, to some key concepts of the Japanese legislation. More specifically, there is a lack of clarity around the **status of the so-called “trustee”**- a term which resembles to the one of the data processor under the GDPR but whose ability to determine and change the purposes and means of processing of personal data remains ambiguous.
22. The EDPB would also need assurances due to lack of the relevant documents, on whether the **restrictions to the rights of individuals** (in particular, rights of access, rectification, and objection) are necessary and proportionate in a democratic society and respect the essence of fundamental rights.
23. The EDPB would also expect that the European Commission closely monitors the effective protection of **personal data transferred from the EU to Japan, based on the draft adequacy decision, throughout their whole “life cycle”** even though the Japanese legislation imposes a record keeping obligation of the origin of the data for a maximum of three years.

1.4 On the access by public authorities to data transferred to Japan

24. The EDPB has also analysed the legal framework for Japanese governmental entities when accessing personal data transferred from the EU to Japan for law enforcement or national security purposes. While acknowledging the reassurances provided by the Japanese government, referred to as the Annex II to the draft adequacy decision, the EDPB has identified a number of aspects for clarifications and of concern, of which the following should be highlighted.
25. In the area of law enforcement, the EDPB notes that the legal principles applying to access data often appear to be similar to the rules in the EU, to the extent they are available. The lack of available translations of several legal texts and of relevant case law make it difficult, however, to conclude that all the procedures for accessing data are necessary and proportionate and that the application of those principles are applied in a way which is “essentially equivalent” to EU law.
26. In the area of national security, the EDPB recognises that the Japanese government has restated that information may only be obtained from freely accessible sources or through voluntary disclosure by companies, and that it does not collect information on the general public. It is aware, however, of concerns expressed by experts and in the media, and would welcome further clarification on surveillance measures by Japanese governmental entities.
27. As to the legal redress of EU individuals, in the area of law enforcement as well as national security, the EDPB welcomes that the European Commission and the Japanese government have negotiated an additional mechanism for EU individuals to provide them with an additional redress avenue, and thereby extending the powers of the Japanese data protection authority. However, a point of concern remains that this new mechanism does not entirely compensate for the shortcomings of oversight and redress under Japanese law. The EDPB thus seeks for further clarifications in order to ensure that this new mechanism does fully compensate those shortcomings.

1.5 Conclusion

28. The EDPB considers that this adequacy decision is of paramount importance. As the first adequacy decision since the entering into force of GDPR, it will constitute a **precedent for future adequacy**

applications as well as **for the review of the adequacy decisions rendered under Directive 95/46⁹**. It is also important to underline that individuals are more and more conscious of the impact of globalisation on their privacy and turn to their supervisory authorities to ensure that adequate guarantees are in place when their personal data are transferred abroad. In light of these implications, the EDPB believes that the European Commission should ensure that there are no shortcomings in the protection offered by the EU-Japan adequacy and that this specific type of adequacy is aligned with the requirements of Article 45 of the GDPR.

29. The EDPB welcomes the efforts made by the European Commission and the Japanese PPC to align as much as possible the Japanese legal framework to the European one. **The improvements** brought in by the Supplementary Rules to bridge some of the differences between the two frameworks are very important and well received.
30. However, following a careful analysis of the Commission's draft adequacy decision as well as of the Japanese data protection framework, the EDPB notices that **a number of concerns, coupled with the need for further clarifications, remain**. Further, this specific type of adequacy combining an existing national framework with additional specific rules also raises questions about its operational implementation. In light of the above, the EDPB recommends the European Commission to address the concerns and requests for clarification raised by the EDPB and provide further evidence and explanations regarding the issues being raised. The EDPB also invites the European Commission to conduct a review of this adequacy finding (at least) every two years and not every four years as suggested in the current draft adequacy decision.

2 INTRODUCTION

2.1 Japan's data protection framework

31. Japan's data protection framework was modernized very recently, in 2017. This framework comprises several pillars, at the centre of which there is a general statutory law, the Act on Protection of Personal Information (APPI). Another important piece of legislation is the Cabinet Order to Enforce the APPI ("Cabinet Order") which specifies certain core principles of the APPI.
32. Based on a Cabinet decision, adopted on 12 June 2018¹⁰ and Article 6 of the APPI, the PPC was given the power to "*take necessary action to bridge the differences of the systems and operations between Japan and the concerned foreign country in view of ensuring appropriate handling of personal information received from each country*"¹¹. The Cabinet decision also suggests that the rules adopted by the PPC supplementing or going beyond those laid down in the APPI would be binding and enforceable on the Japanese business operators¹².
33. Accordingly, the PPC engaged in negotiations with the European Commission and adopted, in June 2018, stricter rules to the ones of the APPI and the Cabinet Order to be applied to data transferred from the EU. These are the Supplementary Rules under the Act on the Protection of Personal Information for the Handling of Personal Data Transferred from the EU based on an adequacy decision,

⁹ Directive No. 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.

¹⁰ The EDPB notes that according to the draft adequacy decision this Cabinet Decision was adopted on 12 June 2018. However, the EDPB was only provided with the draft version of the Cabinet Decision, dated April 2018.

¹¹ Cabinet Decision of April 25th, 2018.

¹² See section 1.3.4 below for more information.

hereafter “Supplementary Rules”¹³. These Supplementary Rules are also annexed to the draft implementing Commission decision published in July 2018.

34. It is important to note that the Supplementary Rules are only applicable to personal data transferred from the European Union to Japan on the basis of the adequacy decision and aim at enhancing the applicable protection to those data. As such they do not apply to personal data of individuals in Japan or coming from other countries than the ones of the EEA.
35. Further, the EDPB would like to draw attention to the fact that the amended APPI came into force on May 30, 2017 and the PPC in its current form was established in 2016. Moreover, the Supplementary Rules negotiated by the PPC with the European Commission have yet to enter into force as that will depend on the recognition by the European Commission of Japan as a jurisdiction adequate to the one in the EU.

2.2 Scope of the EDPB’s assessment

36. The European Commission’s draft adequacy decision is the result of an assessment of the Japanese data protection rules, followed by negotiations with the Japanese authorities. The outcome of these negotiations is notably reflected in the two annexes attached to the draft adequacy decision: the first one provides for additional protections that Japanese business operators will have to apply to the processing of personal data transferred from the EU, while the second one contains assurances and commitments from the Japanese government concerning public authorities’ access to data.
37. The EDPB examined the Japanese data protection framework, the Supplementary Rules negotiated by the European Commission and the assurances and commitments from the Japanese government. The EDPB is expected to provide an independent opinion on the European Commission’s findings, identify insufficiencies in the adequacy framework, if any, and endeavour to propose alterations or amendments to address these.
38. As mentioned in the EDPB adequacy referential, “*the information provided by the European Commission should be exhaustive and put the EDPB in a position to make an own assessment regarding the level of data protection in the third country*”¹⁴.
39. Nonetheless, the EDPB received most of the documents in English translations, referenced in the draft adequacy decision, which form an essential part of the Japanese legal system. The EDPB, therefore, renders the present opinion on the basis of the analysis of available documents in English. The EDPB took into account the applicable data protection framework in the European Union, including Article 8 of the European Convention on Human Rights (hereinafter: ECHR) protecting the right to private and family life as well as Articles 7, 8 and 47 of the Charter of Fundamental rights of the European Union (hereinafter: the Charter) respectively protecting the right to private and family life, the right to protection of personal data and the right to an effective remedy and fair trial. In addition to the above, the EDPB considered the requirements of GDPR as well as looking at the relevant jurisprudence.
40. The objective of this exercise is to ensure that the Japanese data protection framework is essentially equivalent to that of the European Union. The concept of “adequate level of protection” which already existed under Directive 95/46, has been further developed by the CJEU. It is important to recall the

¹³ Supplementary Rules, Annex I of the Commission Implementing Decision of XXXX, pursuant to Regulation 2016/679 of the European Parliament and the Council on the adequate protection of personal data by Japan, sent to the EDPB on September 2018.-

¹⁴ WP254, p.3.

standard set by the CJEU in Schrems, namely that – while the "level of protection" in the third country must be "essentially equivalent" to that guaranteed in the EU – "the means to which that third country has recourse, in this connection, for the purpose of such a level of protection may differ from those employed within the [EU]"¹⁵. Therefore, the objective is not to mirror point by point the European legislation, but to establish the essential and core requirements of the legislation under examination. Adequacy can be achieved through a combination of rights for the data subjects and obligations on those who process data, or who exercise control over such processing and supervision by independent bodies. However, data protection rules are only effective, if they are enforceable and followed in practice. It is therefore necessary to consider not only the content of rules applicable to personal data transferred to a third country or an international organization, but also the system in place to ensure the effectiveness of such rules. Efficient enforcement mechanisms are of paramount importance to the effectiveness of data protection rules¹⁶.

2.3 General comments and concerns

2.3.1 Specificities of this type of adequacy decision

41. The EU-Japan adequacy is the first one to be examined against the new legal backcloth of GDPR. This renders the work of the EDPB all the more important in light of the effects of this draft adequacy decision for future adequacy applications.
42. The EU – Japan adequacy would also be the first mutual one. When and if the EU recognises Japan as providing an essentially equivalent level of protection to the one of the GDPR, Japan will also issue its own adequacy decision under Article 24 of the APPI, recognising the EU as offering an adequate level of protection under the Japanese data protection framework. Thus this envisaged Japan – EU adequacy is of a particular nature which the EDPB has taken into account in its assessment. As mentioned above, the Japanese PPC has negotiated specific, stricter rules with the European Commission, applicable only to personal data transferred from the EU. These stricter rules are binding and enforceable according to the Cabinet Decision and are to be complied with by all Personal Information Handling Business Operators (hereafter PIHBOs) in Japan when processing personal data coming from the EU under this draft adequacy decision.
43. The European Commission has therefore based its adequacy finding not only on the existing general Japanese data protection framework but also on these specific rules. The fact that Supplementary Rules were required to complement the APPI is indicative of the fact that the European Commission acknowledges that the Japanese data protection legislation is not, per se, essentially equivalent to the GDPR.
44. **In light of the above-mentioned issues, the EDPB invites the European Commission to ensure that this new architecture of adequacy, the first to be adopted under the GDPR, relying on Supplementary Rules, will be a sustainable and reliable system that will not raise practical issues regarding the concrete and efficient compliance by Japanese entities and enforcement by the PPC.**

2.3.2 Certainty of translations

45. Like the European Commission, the EDPB has worked on the basis of English translations provided by the Japanese authorities¹⁷. The EDPB calls the European Commission to clarify that it has based its draft adequacy decision on the English translations received and verify the quality and certainty of these translations regularly.

¹⁵ Case C- 362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015 (§§ 73, 74).

¹⁶ WP254, p.2.

¹⁷ The European Commission has verified these translations.

2.3.3 Sectorial Adequacy

46. The adequacy finding of this draft adequacy decision is limited to the protection of personal information by PIHBOs within the meaning of the APPI. This means that the adequacy is sectorial as it only applies to the private sector, excluding from its scope transfers of personal data between public authorities and bodies. Currently, the European Commission briefly mentions this specificity of the scope of the adequacy in recital 10 of the draft adequacy decision.
47. **The EDPB invites the European Commission to explicitly mention the sectorial nature of this adequacy finding in the title of the implementing decision as well as in its Article 1 in accordance with Article 45 (3) GDPR.**

2.3.4 Binding nature of Supplementary Rules and of PPC Guidelines

48. Article 6 of the APPI mentions that “the government shall...take necessary legislative and other action so as to be able to take discreet action for protecting personal information that especially requires ensuring the strict implementation of its proper handling in order to seek enhanced protection of an individual’s rights and interests, and shall take necessary action in collaboration with the governments in other countries to construct an internationally conformable system concerning personal information through fostering cooperation with an international organization and other international framework.” Although the government is clearly identified in this Article of the APPI as competent to take such legal action, it does not refer directly to the PPC as the competent body to adopt specific rules¹⁸. Due to time constraints, the EDPB was unable to gather, review and examine existing evidence on this point.
49. **In light of the importance of this issue, the EDPB takes note of the repeated commitments and reassurances of the European Commission and of the Japanese authorities regarding the binding and enforceable nature of the Supplementary Rules. The EDPB invites the European Commission to continuously monitor their binding nature and effective application in Japan as their legal value is an essential element of the EU – Japan adequacy.**
50. Moreover, the European Commission makes reference in several sections of its draft adequacy decision to the PPC Guidelines (Guidelines).
51. Although the European Commission clarifies that the Guidelines provide an authoritative interpretation of the APPI in recital 16 of its draft adequacy decision, in the same recital it makes reference to the binding nature of these Guidelines: “According to the information received from the PPC, those Guidelines are considered as binding rules that form an integral part of the legal framework, to be read together with the text of the APPI, the Cabinet Order, the PPC Rules and a set of Q&A prepared by PPC.”¹⁹
52. However, the understanding of the EDPB, based on the same information provided by the PPC, is that the Guidelines are not legally binding. Rather, they provide an ‘authoritative interpretation’ of the law. The PPC argues that the Guidelines are followed by PIHBOs in practice, used by the PPC for enforcing

¹⁸ According to an article published in July 2018, when the Supplementary Rules were in a draft, the legal binding nature of these Rules was likely to be the object of internal debate in the country. See Fujiwara S., Comparison between the EU and Japan’s Data Protection Legal Frameworks’, Jurist, vol. 1521 (July 2018): p. 19.

¹⁹ Commission Implementing Decision of XXXX, pursuant to Regulation 2016/679 of the European Parliament and the Council on the adequate protection of personal data by Japan, as sent to the EDPB on November 13, 2018, Recital 16.

the law against PIHBOs and used by courts when rendering their judgment. However, these elements do not constitute sufficient evidence that the Guidelines are legally binding norms.

53. **The EDPB would welcome clarifications in the adequacy decision in relation to the binding nature of the PPC Guidelines and asks the European Commission to attentively monitor this aspect.**
54. According to the PPC, the Guidelines are followed in practice nevertheless as it is local custom. The PPC mentions that the Japanese courts use the PPC Guidelines to render their judgments when applying APPI rules. The European Commission makes reference to a court ruling²⁰ dating from 2006 to provide evidence that the Japanese courts base themselves on guidelines for their findings. Despite the fact that the EDPB was not provided with this court ruling, the EDPB would appreciate if the European Commission could provide, if available, a more recent court ruling, either in the field of data protection or in another sector where the Japanese courts have used the PPC Guidelines or other similar guidelines as a basis of their decision.

2.3.5 Periodic review of the adequacy finding

55. Article 45 (3) of the GDPR provides that a periodic review must take place at least every four years. According to the EDPB adequacy referential²¹, this is a general time frame which must be adjusted to each third country or international organization with an adequacy decision. Depending on the particular circumstances at hand, a shorter review cycle could be warranted. Also, incidents or other information about or changes in the legal framework in the third country or international organization in question might trigger the need for a review ahead of schedule. It also appears to be appropriate to have a first review of an entirely new adequacy decision rather soon and gradually adjust the review cycle depending on the outcome.
56. Taking into account a number of factors, including the fact that the APPI entered into force in 2017, that the PPC was established in 2016 and that there is no information nor evidence on the practical application of the Supplementary Rules yet, **the EDPB invites the European Commission to conduct a review of this adequacy finding (at least) every two years and not every four years as suggested in the current draft adequacy decision.**

2.3.6 International commitments entered into by Japan

57. According to Article 45 (2) (c) of the GDPR and the adequacy referential²², when assessing the adequacy of the level of protection of a third country, the European Commission shall take into account, among others, the international commitments the third country has entered into, or other obligations arising from the third country's participation in multilateral or regional systems in particular in relation to the protection of personal data, as well as the implementation of such obligations. Furthermore the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data ("Convention 108+"²³ and its Additional Protocol should be taken into account.
58. **In this regard, the EDPB notes that Japan is an observer of the Consultative Committee of Convention 108+.**

²⁰ Commission Implementing Decision of XXXX, pursuant to Regulation 2016/679 of the European Parliament and the Council on the adequate protection of personal data by Japan, as sent to the EDPB on November 13, 2018, page 5, footnote 16, "Osaka District Court, decision of 19 May 2006, Hanrei Jiho, Vol. 1948, p. 122.

²¹ WP254, p.3.

²² WP254, p.2.

²³ Convention for the protection of individuals with regard to the processing of personal data, Convention 108+, 18 May 2018.

- 2.3.7 Powers of DPAs²⁴ to bring actions concerning the validity of an adequacy decision before a court
59. The EDPB underlines that although recital 179 of the draft adequacy decision only mentions cases where a DPA has received a complaint questioning the compatibility of an adequacy decision with the fundamental rights of the individual to privacy and data protection, this statement is to be understood as an example of situations, where a DPA can bring the matter before a national court, which could also be possible in the absence of a complaint, rather than as a restriction to the powers provided to DPAs under the GDPR and national laws of the Member States in this regard. Indeed, the provisions of the GDPR include both the power to suspend data transfers even when based on an adequacy decision and to bring an action concerning the validity of an adequacy decision, are not limited to cases where they have received a complaint, should their national law grant them the power to do so more broadly and independently from a complaint, in accordance with the relevant provisions of the GDPR.
60. **The EDPB invites the European Commission to clarify in its draft adequacy decision that the power of supervisory authorities to bring an action against the validity of an adequacy decision following a complaint is just an illustration of the broader powers of DPAs following from the GDPR, which include the power to suspend transfers and to bring an action concerning the validity of an adequacy decision in the absence of a complaint should their national law provide it.**

3 COMMERCIAL ASPECTS

3.1 Content principles

61. Chapter 3 of the Adequacy Referential is dedicated to the “Content Principles”. A third country’s or international organisation’s system must contain them in order to regard the level of protection provided as essentially equivalent to the one guaranteed by EU legislation. The EDPB acknowledges the fact that the Japanese legal system pursues a different approach to that of the GDPR in order to give effect to the right to privacy. Although the right to privacy is not enshrined in the Japanese Constitution per se, it has been recognised as a constitutional right via case law as also referenced in the European Commission’s decision²⁵.
62. Especially due to the fact that the Japanese approach noticeably differs from the European one, it has to be observed carefully whether, not only single aspects, but the system as a whole ultimately provides an “essentially equivalent” level of protection. This means, that potential “shortcomings” concerning one content principle might be compensated by some other aspects providing adequate checks and balances.

3.1.1 Concepts

63. Based on the adequacy referential, basic data protection concepts and/or principles should exist in the third country’s legal framework. Although these do not have to mirror the GDPR terminology, they should reflect and be consistent with the concepts enshrined in the European data protection law. For example, the GDPR includes the following important concepts: “personal data”, “processing of personal data”, “data controller”, “data processor”, “recipient” and “sensitive data”²⁶.

²⁴ Case C- 362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015.

²⁵ The EDPB has not been provided with the English translation of this Court decision. See Commission Implementing Decision of XXXX, pursuant to Regulation 2016/679 of the European Parliament and the Council on the adequate protection of personal data by Japan, as sent to the EDPB on November 13, 2018, footnote 9

²⁶ WP254, p.4.

64. The APPI also includes a number of definitions such as, among others, those of “personal information”, “personal data”, “personal information handling business operator”. **However, it seems that the APPI does not include a definition of the term “handling of personal data” which is similar to the term “processing of personal data”.**
65. Regarding the definition of the term “handling of personal data”, the PPC provided written answers to the EDPB’s question on this definition. The European Commission quoted this answer to the draft Commission decision “*While the APPI does not use the term “processing”, it relies on the equivalent concept of “handling” which, according to the information received by the PPC, covers “any act on personal data” including the acquisition, input, accumulation, organisation, storage, editing/processing, renewal, output, reassurance, output, utilization, or provision of personal information.*”²⁷
66. However, since the text of reference for this definition has not been provided, the EDPB invites **the European Commission to closely monitor that the definition of the abovementioned concept, as provided by the PPC, is effectively followed in practice.**
- 3.1.1.1 Concept of data processor and obligations of a “trustee”*
67. As mentioned above, the adequacy referential requires that basic data protection concepts and/or principles should exist in the third country’s legal framework.
68. The APPI includes a definition of a “personal information handling business operator” which according to the European Commission comprises both the terms of a data controller and a data processor as provided by the GDPR and does not distinguish between the two²⁸. However, the APPI also includes a term “trustee” in its Article 22, which in some ways resembles the term of a data processor under the GDPR.
69. As explained by the PPC in its answers provided to the EDPB, and also included in the European Commission’s draft adequacy decision, a trustee is considered as the equivalent of a data processor under the GDPR – entrusted with the handling of personal data by a PIHBO. This trustee has the same obligations and rights as any PIHBO, including the ones of the Supplementary Rules for personal data transferred from the EU. The PIHBO that entrusts the handling of personal data to a trustee is bound to “exercise necessary and appropriate supervision”²⁹ over the trustee.
70. **The EDPB invites the European Commission to explain the trustee’s status and obligations when the trustee changes the purposes and means of processing and clarify whether the data subject’s consent remains a necessary condition for such change of purpose or determination of means³⁰.**

²⁷ Commission Implementing Decision of XXXX, pursuant to Regulation 2016/679 of the European Parliament and the Council on the adequate protection of personal data by Japan, as sent to the EDPB on November 13, 2018, recital 17.

²⁸ Commission Implementing Decision of XXXX, pursuant to Regulation 2016/679 of the European Parliament and the Council on the adequate protection of personal data by Japan, as sent to the EDPB on November 13, 2018, recital 35.

²⁹ Article 22 of the Amended Act on the Protection of Personal Information (APPI), put into effect on May 30, 2017.

³⁰ Art. 23 para 5 (i) APPI. See also section on the transparency principle below.

3.1.1.2 Concept of retained personal data

71. The APPI contains the concept of “retained personal data” which is considered to be a sub-category of personal data. According to the APPI, the provisions relating to the data subject’s rights³¹only apply to retained personal data. The definition of retained personal data is included in Article 2(7) of the APPI.
72. Retained personal data are the personal data other than those that (i) are set to be deleted within a period of no longer than 6 months³² or that (ii) fall under the exceptions of Article 4 of the Cabinet Order and that are likely to harm the public or other interests if their presence or absence is made known.
73. The Supplementary Rule (2) provides that “*personal data received from the EU based on an adequacy decision is required to be handled as retained personal data irrespective of the period within which it is set to be deleted.*”
74. However, personal data falling under the exceptions of Article 4 of the Cabinet Order will not be required to be handled as retained personal data and that data subject rights will not apply.
75. Article 23 of the GDPR provides that, like Article 4 of the Cabinet Order, Union or Member State law to which the data controller/processor is subject to, may restrict the scope of the obligations applicable to him and the rights available to the data subject. This can be done by way of a legislative measure. These restrictions need to respect the essence of the fundamental right and freedoms and is a necessary and proportionate measure in a democratic society.
76. Regarding the substance of the exceptions provided for in Article 4 of the Cabinet Order, the EDPB has not been provided with sufficient documentation on these limitations or additional elements to clarify the scope of these provisions³³. The EDPB is not in a position to assess whether these limitations to the rights of data subjects are limited to what would be considered strictly necessary and proportionate under EU law, and would thus be essentially equivalent to the rights provided to the EU data subjects.
77. **Due to lack of some relevant documents, the EDPB would also welcome reassurances by the European Commission, if restrictions to the rights of individuals (in particular, rights of access, rectification and objection) are necessary and proportionate in a democratic society and respect the essence of fundamental rights.**
78. An essential requirement under the GDPR is that personal data are protected throughout their whole “life cycle”.
79. Taking into account the fact that the Supplementary Rules only apply to personal data transferred from the EU, the EDPB would appreciate receiving further information about the practical implementation of these rules by PIHBOs, especially when these data are further communicated to another PIHBO after their first transmission to Japan.
80. The European Commission has clarified in recital 15 of its draft adequacy decision that PIHBOs receiving and/or further processing personal data from the EU will be under a legal obligation to comply with the Supplementary Rules and that in order to do so they will need to ensure that they can identify such personal data throughout their “life-cycle”.

³¹ Articles 27-30 of the APPI.

³² Amendment to the Cabinet Order to Enforce the Act on the Protection of Personal Information (Cabinet Order), put into effect May 30, 2017, Article 5.

³³ The EDPB has not been provided with the Supreme Court decisions referred to in recital 53 of the draft adequacy decision.

81. In its answers, The PPC³⁴has explained that such identification will be made by using technical methods (tagging) or organisational methods (storing the data originating from the EU in a dedicated database).
 82. In footnote 14 of its draft adequacy decision, the European Commission explains that PIHBOs must record the information on the origin of the EU data for as long as necessary in order to be able to comply with the Supplementary Rules. This is also enshrined in Article 26 (1), (3) and (4) of the APPI which states that a PIHBO is under the obligation to confirm and record the source of these data and all the circumstances surrounding the acquisition of these data.
 83. However, the EDPB notes that Article 18 of the PPC Rules³⁵ specifies that the record keeping obligations of PIHBOs are limited to a maximum of three years for cases that fall outside the specific record keeping methods described in Article 16 of the PPC Rules (using a written document, electromagnetic record or microfilm). This is also stated by the European Commission in recital 71 of its draft adequacy decision: "*As specified in Article 18 of the PPC Rules, those records must be preserved for a period of one to three years, depending on the circumstances*".
 84. Even if, as the European Commission states in footnote 14 of its draft adequacy decision, PIHBOs are not prohibited to keep records regarding the origin of the data for longer than three years, in order to be able to fulfil their obligations under Supplementary Rule (2), this is neither clearly reflected in the Japanese legislation nor in the Supplementary Rules. The EDPB considers that there is a risk that PIHBOs will in fact comply with Article 18 of the PPC Rules even when they process data originating from the EU. This is mainly because there is currently, to the understanding of the EDPB and based on available documents, no provision putting PIHBOs under such an obligation to comply with the Supplementary Rules instead. This would result in data transferred from the EU to no longer being protected by the additional protections included in the Supplementary Rules.
 85. **The EDPB invites the European Commission to closely monitor the effective protection of personal data transferred from the EU to Japan based on the draft adequacy decision, throughout their whole life-cycle even though the Japanese legislation imposes a record keeping obligation of the origin of the data for a maximum of three years.**
- 3.1.2 Grounds for lawful and fair processing for legitimate purposes
86. According to the adequacy referential, in line with the GDPR, data must be processed in a lawful, fair and legitimate manner³⁶. The legal basis, under which personal data may be lawfully, fairly and legitimately processed, should be set out in a sufficiently clear manner. The European framework acknowledges several such legitimate grounds including, for example, provisions in national law, the consent of the data subject, performance of a contract or legitimate interest of the data controller or of a third party which does not override the interests of the individual.
 87. Under the APPI, consent plays a central role in the Japanese data protection legal system. Consent is the central legal basis for the processing of personal data in Japan, and also one of the main legal basis for transfers of personal data from Japan to a third country. In addition, consent is required for an alteration of the purpose of the processing.
 88. According to Supplementary Rule (3), the legal basis for the processing of personal data transferred from the EU to Japan will be the legal basis for which the data is transferred to Japan. If the PIHBO

³⁴ Annex III of the present Opinion.

³⁵ Enforcement Rules for the Act on the Protection of Personal Information (PPC Rules), put into effect May 30, 2017, Article 16.

³⁶ WP254, p.4.

wishes to process further these data for a different purpose he needs to obtain the consent of the data subject in advance.

89. The EDPB considers that the quality of consent, especially due to its central role in the Japanese legal framework, has to comply with the fundamental requirements of the notion of consent, i.e. according to EU law, a “*freely given, specific, informed and unambiguous indication of the data subject’s wishes...*”. The data subject can withdraw such consent as an essential safeguard to ensure the free will of the data subject throughout the time³⁷. The right to withdrawal, as a mandatory element of consent, appears to be missing in the Japanese legal framework. Indeed, according to the PPC guidelines³⁸ the withdrawal is merely “desirable” and conditional to the “characteristics, size and the status of the business activities”.

3.1.3 The transparency principle

90. Based on Article 5 of the GDPR, transparency is a fundamental principle of the EU data protection system³⁹. The adequacy referential explicitly names “transparency” as one of the content principles to be taken into account when evaluating the essentially equivalent level of protection provided for by a third country. The transparency and fairness principle strives to ensure that the data subject has control over his/her data and, for this purpose, information shall be provided to the data subject in a proactive manner as a rule. In the case of the Privacy Shield, the Article 29 Working Party⁴⁰ in their opinion 1/2016 made reference to Annex II, II 1 b of the Privacy Shield agreement (notice to the individual) and stated that, if the data is not collected directly, an organisation should notify the data subject “at the point the data is recorded by the Shield organisation” (section 2.2.1.a). Having the privacy policy publicly available is an additional criterion (see section 2.2.1.b). Hence, already under Directive 95/46/EC it was deemed necessary to directly inform the data subject.
91. A first concern is raised regarding the modality of information provided to the data subject under the APPI. According to Article 27 (1) of the APPI, a PIHBO is obliged to provide the information described in Article 27 (1) APPI by putting it “into a state where a principal can know”. However, this wording does not make clear to what extent the PIHBO has to take positive measures to genuinely inform the data subject.
92. **The EDPB invites the Commission to clarify the meaning of the term “can know” and whether the APPI provides as a rule the obligation to genuinely inform data subjects.**
93. Moreover, according to the adequacy referential, restrictions to the information to be provided to the data subject may exist, similar to Article 23 GDPR. On a similar vein, Article 14 (5) of the GDPR provides for an exception to the right to be informed when the information is likely to render impossible or seriously impair the achievement of the processing. However, even in this case, the controller shall provide some sort of information as, for instance, by making “generalised” information publicly

³⁷ GDPR, Article 4(11). For more information see also relevant guidelines of the EDPB on consent WP259, 10 April 2018.

³⁸ Data Protection Legal and Technical Research and Analysis Consortium (DPC), An assessment of the level of protection of personal data provided under Japanese law, p. 46: “Further, from the viewpoint of protection of rights and interests of a principal such as consumers, it is desirable, in case of having received a demand from a principal for the retained personal data, to further respond to the principal’s demand in such a way as stopping etc. of direct-mail sending or voluntarily fulfilling a utilisation cease etc. considering the characteristics, size and the status of the business activities”.

³⁹ WP 254, chapter 3, point 7, p. 5; see also recital (39) GDPR.

⁴⁰ This Working Party was set up under Article 29 of Directive 95/46/EC. It was an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. The WP29 has now become the EDPB.

available. Moreover, when the risk ceases to exist the data subject shall be notified⁴¹. These aspects are important in order to ensure the fundamental principle of fairness.

94. Under Article 23 of the APPI, a PIHBO generally has to give in advance information to the data subject about providing his/her data to a third party either implicitly when obtaining his/her consent or explicitly by an opt-out notification. The EDPB understands that there is no notification to the data subject, informing him/her of the fact that his/her data are not retained personal data under the APPI because falling under the exceptions of Article 4 of the Cabinet Order. As a result, they will not be able to benefit from their rights in full. The data subjects are not informed in the cases of Article 18(4) APPI either.
95. **The EDPB acknowledges that the rights may be restricted for legitimate objectives pursued by the PIHBO and the state authorities. At the same time, the EDPB considers that there should be at least a general information upfront on the possibility of the restriction of the rights for the objectives referred to the law and that the data subject should be notified when the risks for which the information is restricted cease to exist.**
96. Finally, other aspects of transparency are developed further below. These refer to the risks the transfer to a third country entails⁴² and the information on the logic of processing in the context of automated decision making, including profiling.⁴³

3.1.4 Restrictions on onward transfers

97. The EDPB welcomes the efforts made by the Japanese authorities and the European Commission to enhance the level of protection for onward transfers in Supplementary Rule (4), which excludes that personal data transferred from the EU is further transferred to a third country on the basis of APEC-CBPRs. In addition, the EDPB recognises that in recitals 177 and 184 of its new draft of the adequacy decision, the European Commission committed itself to suspend the adequacy decision when onward transfers no longer ensure the continuity of protection. However, the EDPB would like to raise two points regarding these transfers of EU personal data from Japan to third countries.
98. **The use of consent as a basis for data transfers from Japan to a third country in the Japanese legal system raises concerns as the EDPB considers that the information given to the EU data subject prior to consenting seems not to be comprehensive.**
99. Article 24 APPI prohibits the transfer of personal data to a third party outside the territory of Japan without the prior consent of the individual concerned. Supplementary Rule (4) stipulates that EU data subjects have to be provided with information on the circumstances surrounding the transfer necessary to make a decision on his/her consent.
100. The European Commission concludes in its draft adequacy decision that Supplementary Rule (4) secures a particular well informed consent of the EU data subject⁴⁴ as he/she will be advised of the fact that the data will be transferred abroad and of the specific country of destination. This would allow the data subject to assess the risk for privacy involved with the transfer.

⁴¹ Tele2, Joined Cases C 203/15 and C 698/15, judgement of the Court, 21 December 2016, rec. 121 and Digital Rights Ireland, Joined Cases C-293/12 and C-594/12, judgement of the Court, 8 April 2014, rec. 54-62.

⁴² See section 2.1.4.

⁴³ See section 2.1.6.

⁴⁴ Commission Implementing Decision of XXXX, pursuant to Regulation 2016/679 of the European Parliament and the Council on the adequate protection of personal data by Japan, as sent to the EDPB on November 13, Recital 76.

101. Under the transparency principle of the adequacy referential, a certain degree of fairness shall be ensured when informing individuals. In the context of onward transfers based on consent, the EDPB is of the opinion that to ensure such adequate degree of fairness data subjects should be explicitly informed about the possible risks of such transfers arising from the absence of adequate protection in the third country and the absence of appropriate safeguards prior to consent. Such notice should include for example information that in the third country there might not be a supervisory authority and/or data processing principles and/or data subject rights might not be provided for in the third country⁴⁵. For the EDPB the provision of this information is essential in order to enable the data subject to consent with full knowledge of these specific facts of the transfer⁴⁶.
102. Informed consent is also important regarding sectorial exclusions. The adequacy decision does not cover certain types of processing by certain bodies such as universities for the processing of personal data for academic purposes. The EDPB's concern here relates to the specific scenario of when data transferred from the EU under the adequacy decision – for example the HR data of Erasmus students in Japan – are then used for a different purpose falling out of the scope of the adequacy decision (e.g. research purposes), with the consent of the data subject, - and are therefore no longer covered by the additional protection provided by the Supplementary Rules.
103. The European Commission states in recital 38 of its draft adequacy decision that such a scenario will fall under the context of onward transfers and that, where this takes place, the PIHBO has to provide the data subject with all the necessary information before obtaining his/her consent, including that the personal information would not fall under the protection of the APPI rules.
104. Supplementary Rule (4) only requires the PIHBO to obtain the data subject's consent after having been provided with information on the circumstances surrounding the transfer necessary for the principal to make a decision on his/her consent.
105. **The EDPB invites the European Commission to ensure that the information to be provided to the data subject “on the circumstances surrounding the transfer” should include the information about the possible risks of transfers arising from the absence of adequate protection in the third country and the absence of appropriate safeguards, or in the case of sectorial exclusions, of the absence of protections of the Supplementary Rules and of the APPI.**
106. **Onward transfers of personal data may occur to third countries, which become subject to a possible later Japanese adequacy decision.**
107. Without prejudice to the derogations set forth in Article 23 para 1 of the APPI, data initially transferred from the EU to Japan can be then transferred from Japan to a third country without consent in two cases:
 - If the PIHBO and the third party recipient have together implemented measures providing a level of protection equivalent to the APPI read together with the Supplementary Rules by means of a contract, other forms of binding agreements or binding agreements within a corporate group⁴⁷.

⁴⁵ EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25 May 2018, p.8.

⁴⁶ EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25 May 2018, p.7.

⁴⁷ Supplementary Rule (4) (ii).

- If the third country has been recognised by the PPC under Article 24 of the APPI and Article 11 of the PPC Rules⁴⁸ as providing an equivalent level of protection to the one guaranteed in Japan.
108. The EDPB evaluates Article 24 APPI as the more specific rule, which contains a derogation from the general rule under Article 23 APPI. Therefore, the EDPB does not share the European Commission's assessment in the new last sentence of Recital 78 of the draft adequacy decision stating that even in those cases, the transfer to the third party remains subject to the requirement to obtain consent under Article 23 (1) of the APPI.
109. Pursuant to Article 11 (1) of the PPC Rules, an adequacy decision by the PPC requires substantive standards equivalent to the APPI whose implementation are ensured in the third country and which are effectively supervised by an independent enforcement authority. Moreover, the PPC may impose necessary conditions to protect the rights and interests of individuals in Japan, according to Article 11 (2) of the PPC Rules.
110. Supplementary Rule (4) states that EU personal data can be transferred to a third country subject to a Japanese adequacy decision without further restrictions. But Article 44 of the GDPR regulates that any transfer of personal data to a third country has to fulfil the conditions laid down in Chapter V of the GDPR including onward transfers from the third country to another third country. The level of protection of natural persons whose data is transferred must not be undermined by the onward transfer⁴⁹. Although this interpretation is in principle also shared by the European Commission in its draft adequacy decision⁵⁰, it seems not to be completely followed. The European Commission has negotiated the prohibition of data originating from the EU being transferred to a third country on the basis of Asia Pacific Economic Cooperation (APEC) – Cross Border Privacy Rules (CBPRs). In the light of the comparative tool developed in 2014 under the framework of the EU Directive between BCR and CBPR showing the requirements of both systems, their convergences and differences (WP29 Opinion 02/2014), the EDPB has concerns about the use of CBPRs as an onward transfer tool for personal data transferred from the EU to countries outside of Japan.
111. In contrast, onward transfers of personal data transferred from the EU to Japan on the basis of a Japanese adequacy decision, seem to be accepted by the European Commission, without the possibility for the PPC to impose the Supplementary Rules as conditions to protect the rights and interests of EU individuals, if necessary. The EDPB deduces from Article 44 of the GDPR that the enhanced protection of data being transferred from the EU to Japan foreseen in the Supplementary Rules has always to be extended when personal data transferred from the EU to Japan is further transferred to a third country, if the data protection framework in that country is not recognised as essentially equivalent to the GDPR.
112. **Hence, the EDPB invites the European Commission to take over its monitoring role and to ensure the level of protection of EU data is maintained or to consider suspension of this adequacy decision if personal data transferred from the EU to Japan is further transferred to third countries subject to a**

⁴⁸ Enforcement Rules for the Act on the Protection of Personal Information, 30 May 2017. An English translation of the new Article 11 was communicated by the EU Commission to the EDPB, but this Article has not been published yet.

⁴⁹ WP 254, p.5.

⁵⁰ Commission Implementing Decision of XXXX, pursuant to Regulation 2016/679 of the European Parliament and the Council on the adequate protection of personal data by Japan, as sent to the EDPB on November 13, Recital 75.

possible later Japanese adequacy decision, when these third countries have not been subject of a previous assessment or adequacy finding of the EU.

3.1.5 Direct marketing

113. According to Supplementary Rule (3), a PIHBO is prohibited from processing the data for the purpose of direct marketing if it has been transferred from the European Union for another purpose and the EU data subject has not given his or her consent to the change of the utilisation purpose.
114. According to the Adequacy referential where data are processed for the purposes of direct marketing, the data subject should be able to object without any charge from having his/her data processed for such purposes at any time. According to Article 16 of the APPI, a PIHBO is only allowed to process personal information if the data subject gives his or her consent. The withdrawal of consent could provide the same result as the privileged right to object to direct marketing.
115. The Japanese data protection framework does not provide a privileged right of objection and as explained above in the section on consent, withdrawal of consent under the PPC Guidelines is merely desirable and conditional and can therefore not be considered to equate to a right to object at any time as requested under the Adequacy referential. **The EDPB invites the European Commission to provide reassurances about the right to withdrawal of consent and to monitor cases regarding direct marketing.**

3.1.6 Automated decision making and profiling

116. According to the adequacy referential, decisions based solely on automated processing (automated individual decision-making), including profiling, which produce legal effects or significantly affect the data subject, can take place only under certain conditions established in the third country legal framework. Therefore, every time automated decision making and profiling under the aforementioned circumstances is conducted, there has to be a legal ground for this.
117. In the European framework, the conditions for automated decision making include, for example, the need to obtain the explicit consent⁵¹ of the data subject or the necessity of such a decision for the conclusion of a contract. If the decision does not comply with such conditions as laid down in the third country legal framework, the data subject should have the right not to be subject to it. Furthermore, the law of the third country should, in any case, provide for necessary safeguards, including the right to be informed about the specific reasons underlying the decision and the logic involved to correct inaccurate or incomplete information and to contest the decision where it has been adopted on an incorrect factual basis.
118. The Commission decision only refers to banking sector where sectoral rules⁵² regarding automated decisions would apply. The Comprehensive Guidelines for Supervision over Major Banks mentioned in recital 93 of the draft adequacy decision indicate that the concerned individual has to be provided with specific explanations on the reasons for the rejection of a request to conclude a loan agreement.
119. The argumentations of the European Commission referring to the draft adequacy decision (Recital 94), that the absence of specific rules on automated decision making in the APPI is unlikely to affect the level of protection seems (for instance) do not to take into account the case in which an EU-transferred

⁵¹ For critical remarks to the concept of consent in the Japanese data protection legal framework see: 2.1. General and 2.2.8. Direct marketing.

⁵² These Sectoral Rules were not provided to the EDPB.

personal data is subsequently processed by another Japanese data controller (different from the original Japanese data importer).

120. It appears therefore, that there are no general rules applicable across sectors in Japan governing automated decision making and profiling.
121. **The EDPB invites the European Commission to monitor cases related to automated decision making and profiling.**

3.2 Procedural and enforcement mechanisms

122. Based on the criteria set in the adequacy referential, the EDPB has analysed the following aspects of the Japanese data protection and legal framework as covered under the draft adequacy decision: the existence and effective functioning of an independent supervisory authority; the existence of a system ensuring a good level of compliance and a system of access to appropriate redress mechanisms equipping EU individuals with the means to exercise their rights and seek redress without encountering cumbersome barriers to administrative and judicial redress.
123. Building on the parameters established by the CJEU in the Schrems case⁵³ and those outlined in recital 104 and Article 45 of the GDPR, the EDPB finds that, although a system consistent with the European one exists in Japan, this system may be difficult to access in practice for EU individuals, whose data will be transferred under this adequacy decision in light of the existence of language and institutional barriers.
124. The sections below will examine the above mentioned aspects of the Japanese framework before highlighting some recommendations for the Commission.

3.2.1 Competent independent Supervisory Authority

125. The PPC was established on the 1 January 2016 following the amendments of the APPI of 2015, replacing its predecessor – the Specific Personal Information Protection Commission (established in 2013 under the My Number Act). Although a young organization, since its establishment, the PPC has put considerable efforts into building the required infrastructure to accommodate the implementation of the amended APPI. Noticeable among these are the establishment of the PPC's rules, the PPC Guidelines to give guidance to PIHBOs on the interpretation of the APPI, the publication of a PPC Q&A⁵⁴ document and the setting up of a helpline to advise business operators and citizens on data protection provisions as well as of a mediation service to handle complaints.
126. The establishment and functioning of the PPC is regulated in chapter V of the APPI. Although the PPC falls within the jurisdiction of the Prime Minister, article 62 mandates that the PPC exercises its function independently. The EDPB welcomes the clarification made by the European Commission in the amended draft of the adequacy decision circulated on 13 November 2018 to further describe the degree to which the PPC is free from internal and external influences.

3.2.2 The data protection system must ensure a good level of compliance

127. The draft adequacy decision undertakes a comprehensive examination of the powers that the PPC is equipped with under Articles 40, 41 and 42 of the APPI to ensure the monitoring and enforcement of the legislation. Article 40 empowers the PPC to request PIHBOs to submit reports and documentation relating to processing operations as well as to carry out on-site inspections. Under Article 42, the PPC has the power – when recognising that it is necessary to protect individual rights or where finding a

⁵³ Case 362/14 (2015) Maximilian Schrems v Data Protection Commissioner, (para. 73 and 74).

⁵⁴ This document was not provided by the European Commission to the EDPB in English.

violation of the provisions of the law – to issue recommendations and, those failing, orders to PIHBOs to suspend the act of violation or take necessary measures to rectify the violation.

128. In October 2018, the PPC took one of its first actions under article 41 of the amended APPI and issued ‘guidance’ to a PIHBO, advising the company to strengthen its’ security measures and to effectively supervise applications providers whilst giving clear and easy to understand explanations to users on how their personal information is used, and obtain consent beforehand when the information is shared with a third party as well as respond properly to users’ request for erasure of their information. In the answers provided to the EDPB⁵⁵, PPC officials advised that the company has announced it will cooperate and that, when the company fail to do so, it will render the company with a ‘recommendation’ under Article 42(1) of the APPI.
129. The investigation conducted by the PPC on the above mentioned PIHBO is a very positive indicator of the Japanese supervisory authority’s efforts to ensure a good level of compliance in the country.
130. Although there are improvements in respect to the framework in place prior to the 2015 amendments, the EDPB notices that the PPC has fewer powers than European DPA under the GDPR, especially in relation to **enforcement**. Administrative fines⁵⁶, for example, are quite mild. The European Commission’s decision emphasises in recital 108 that, in cases of non-compliance or some violations of the APPI, criminal sanctions are in place and that the PPC Chair may forward cases to the public prosecutor. However, the European Commission’s decision does not account for the fact that public prosecution in Japan is discretionary and may sometimes be subject to lengthy review processes⁵⁷. In addition, the penalty of imprisonment (with or without labour) associated with violations of the APPI pursuant the provisions in Chapter VII may be difficult to execute because directed at natural persons and, in any case, not punishing the PIHBO as a legal entity failing to exercise its accountability obligations.
131. **In light of the above, the EDPB invites the European Commission to closely monitor the effectiveness of sanctions and relevant remedies in the Japanese data protection system.**
 - 3.2.3 The data protection system must provide support and help to individual data subjects in the exercise of their rights and appropriate redress mechanisms

132. The PPC provides extensive information and guidelines on its website aimed at raising awareness among PIHBOs in relation to their obligations and responsibilities under the data protection framework as well as a Helpline to provide information and support to Japanese citizens regarding their individual rights under the APPI. The website has also a section, called the ‘Children’s room’, explicitly aimed at a children’s and young people audience. The EDPB observes that this information – along with the Helpline support, guidance and Q&A documentations – is available in Japanese⁵⁸. Therefore, the EDPB strongly believes, it would be beneficial if the PPC could provide a dedicated page on the English version of its website aimed at providing information about their individual rights under the Japanese

⁵⁵ Annex III.

⁵⁶ These are provided in Chapter VII of the APPI. The maximum penalty is provided by art. 83 (provision or use by stealth of a personal information database for own or a third party’s illegal profit) and is equivalent to either a year’s imprisonment with work or a fine not exceeding 500,000 yen (roughly EUR 3900). According to the explanations provided by the Commission, fines are cumulative per infringement. Although this may be the case, the EDPB observes that, even if cumulative fines are applied, the total amount is likely to remain considerably low compared to European standards.

⁶⁵ Oda H., Japanese Law, Oxford University Press (III edition), 2009: 439 – 440.

⁵⁸<https://www.ppc.go.jp/en/contactus/piinquiry/>.

data protection framework and under the Supplementary Rules to EU individuals whose data will be transferred to Japan under the European Commission's adequacy decision.

133. The EDPB welcomes the clarification made by the European Commission in recital 104 of the amended draft adequacy decision circulated on 13 November 2018 regarding the mediation service managed by the PPC pursuant Article 61(ii) of the APPI. However, the EDPB would like to raise three points in relation to this. Firstly, the mediation service is not publicized on the English version of the PPC's website. Secondly, the service is accessible only via phone and available in Japanese. Finally, mediation is merely a facilitative process not leading to a binding agreement between the parties which has implications for the effectiveness of the redress options available to data subjects⁵⁹.
134. Finally, the EDPB notices that the draft adequacy decision places emphasis on the remedies available through civil law action as well as criminal proceedings, but does not acknowledge the existence of **institutional barriers to litigation** in Japan such as legal costs (legal fees are split equally between plaintiff and defendant, regardless of which party wins the proceedings⁶⁰), dearth of lawyers in the country⁶¹, the fact that foreign lawyers are not allowed to practice domestic law as well as the burden of proof requirement under Tort Law. The EDPB fears that these factors may – in practice – hinder individuals' access to justice and jeopardise their right to pursue legal remedies rapidly and without bearing prohibitive costs.
135. In light of the above, **the EDPB is concerned that there is a risk that EU individuals may have difficulties accessing administrative and judicial redress** and, therefore, would welcome if the European Commission could discuss with the PPC the possibility of setting up an online service, at least in English, **aimed at providing support to, and handle complaints of⁶², EU individuals**. In addition, the EDPB would welcome the possibility of allowing EU DPAs to act as intermediaries for EU data subject complaints with organisations operating in Japan and the PPC.

4 ON THE ACCESS BY PUBLIC AUTHORITIES TO THE DATA TRANSFERRED TO JAPAN

136. The intention of the COM is to recognise, through the adequacy decision, that "Japan ensures an adequate level of protection for personal data transferred from the European Union to personal information handling business operators in Japan", as stated in Art. 1 of the draft adequacy decision. In line with Art. 45 (2) GDPR, the COM has also analysed the limitations and safeguards as regards access to personal data by public authorities. This chapter focuses on the assessment of the access to personal data by law enforcement authorities and by other government entities for the purpose of national security. The analysis of the EDPB is based on the draft adequacy decision, its Annex II, in which the Japanese government provides an overview of the relevant legal framework, and the Japanese legal texts, to the extent they were provided by the COM. Therefore, in the specific context of this assessment, the EDPB has taken into account elements concerning Japanese laws which are not

⁵⁹ Kojima T., *Civil Procedure and ADR in Japan*, Chuo University Press, 2004; and Menkel-Meadow C., *Dispute Processing and Conflict Resolution: Theory, Practice and Policy*, Ashgate (2003) (ed.).

⁶⁰ Wagatsuma (2012), 'Recent Issues of Cost and Fee Allocation in Japanese Civil Procedure' in Reimann (ed.), *Cost and Fee Allocation in Civil Procedure – Ius Gentium; comparative Perspectives on Law and Justice* Vol. 11, pp. 195 – 200.

⁶¹ According to the latest figures, the number of lawyers in Japan is 38,980 (roughly 290 layers per one million people [Japan Federation of Bar Association] (2017), White Paper on Attorneys: p. 8 – 9.

⁶² Similar to the one envisaged in Annex II of this adequacy decision for complaints from EU residents regarding access to their data by Japanese public authorities.

part of the findings by the European Commission, but that are relevant to assess the conditions and safeguards under which Japanese public authorities are allowed to access personal data transferred from the European Union.

4.1 Law enforcement access to data

4.1.1 Procedures for accessing data in the field of criminal law

137. The draft adequacy decision presents three ways foreseen under Japanese law for law enforcement authorities to access data in Japan:

4.1.1.1 *Access requests with a court warrant*

138. The draft adequacy decision states that for government access in Japan, and especially for criminal law enforcement authorities to request access to electronic evidence in the context of criminal investigations, they always need to have a warrant, unless they use the voluntary disclosure procedure – see below.

4.1.1.1.1 Requirement of “adequate cause”, necessity and proportionality of the warrants

139. The EDPB acknowledges that under the Japanese constitution any collection of personal data by compulsory means must be based on a court warrant. More specifically, the draft adequacy decision indicates that in all cases of “searches and seizures”, court warrants have to be issued for “adequate cause”, which the Supreme Court considers only exists where the individual concerned (suspect or accused) is considered to have committed an offence and the search and seizure is necessary for the criminal investigation. The COM here references the Supreme Court judgment of 18 March 1969, case N. 100 (1968(Shi)).). The EDPB recalls that under the CJEU’s case law⁶³ only a court, and not prosecutors for instance, can authorize the collection of traffic and location data in particular.

140. Also in light of the CJEU jurisprudence, according to which access to data may be subject to a warrant, as in Tele2, the EDPB regrets that no additional information were provided in order to assess how the criteria for assessing the necessity of a warrant – gravity of the offense and how it was committed ; value and importance of the seized materials as evidence ; probability of concealment or destruction of seized materials ; extent of the disadvantages caused by a seizure ; other related conditions – and the concept of “adequate cause” derived from the Constitution are applied in practice. Therefore, the EDPB invites the Commission to monitor if the issuing of warrants meets the criteria set out by the CJEU in practice.

4.1.1.1.2 Types of crimes for which warrants can be issued

141. The warrant procedure applies only whenever a “compulsory investigation” is carried out. In principle, these warrants can only be issued in cases where a violation of law has occurred. In this respect, the EDPB notes the recently adopted “Act on Punishment of Organized Crimes and Control of Crime Proceeds” on 15 June 2017 in the context of adherence of Japan to the UN international Convention on Transnational Crime (UNTOC)⁶⁴. In the absence of an English available version of this legislation, and given the requirement under EU law that some data are collected only in the context of investigation, detection or prosecution of serious crimes⁶⁵, as well as given concerns expressed by several commentators, including UN Special Rapporteur Joseph Cannataci⁶⁶, concerning the wide scope of application, and which relies on a definition of “organized criminal group” reportedly vague

⁶³ See cases 203/15 and C 293/12 and C 594/12 of the CJEU.

⁶⁴ See: <https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html>.

⁶⁵ See joint cases C 293/12 and C 594/12 and case C 203/15.

⁶⁶ UN Special rapporteur on the right to privacy, as well as Graham Greenleaf, UNSW Law Researcher.

and too broad, the EDPB is not in a position to conclude that access to electronic evidence under the relevant Japanese legislation is limited to the thresholds provided by EU law.

142. It has also to be noted that for some types of offences, the Prefectural Police is competent and that they have their specific police ordinances. The internal rules applicable to the Prefectural police were not available to the EDPB.
143. According to the draft Adequacy decision, the collection of electronic information in the area of criminal law enforcement falls under the responsibility of the Prefectural Police.

4.1.1.2 Wiretapping warrants

144. Annex II of the draft adequacy indicates that the Act on Wiretapping for Criminal Investigation provides for specificities for the interception of communications. This legislation was provided very late which did not allow for an in-depth analysis. Therefore, although many safeguards seem to be provided within this legal framework, the EDPB is not in a position to assess whether the conditions provided in this piece of legislation are surrounded by guarantees substantially equivalent to those required in the EU both by the Charter as interpreted by the CJEU and by the ECHR as interpreted by the Strasbourg Court.

4.1.1.3 The “voluntary disclosure” procedure based on enquiry sheet

145. This non-compulsory form of cooperation allows public authorities to ask controllers (except telecommunications carriers) to provide them with data they have. Non-compliance with the request cannot be enforced. It remains unclear which authorities can use this type of procedure, but it appears limited to those investigating crimes.

4.1.1.3.1 Conditions to issue “enquiry sheets”

146. The EDPB acknowledges that the Japanese Supreme Court, by reference to the Constitution, has framed limitations to the use “voluntary disclosures”⁶⁷. It appears from the draft adequacy decision that concretely a “voluntary disclosure” may only be asked by the competent authorities through the issuance of an “enquiry sheet”. Sending such an “enquiry sheet” is said to be permissible only as part of a criminal investigation, and thus to always presuppose a concrete suspicion of an already committed crime. Such investigations are generally carried out by the Prefectural Police, where the limitations pursuant to Article 2(2) of the Police Law apply, which means it should be relevant for the Police activities. However, the EDPB seeks further clarification as to the concrete contours of the criteria allowing to issue an enquiry sheet (such as case law illustrating the application of these criteria), and the relationship between the voluntary disclosure procedure and the seizure of data on the basis of a warrant. Indeed, it appears that even where data could not be obtained through the voluntary procedure, they could still be obtained with a warrant if indispensable for the investigative authorities⁶⁸.

4.1.1.3.2 Available case law on the limitations to the use of voluntary disclosure

147. The cases quoted in the draft adequacy decision⁶⁹ to illustrate limitations to the use of voluntary disclosure procedures relate to cases, where the accused person was either photographed or filmed in the public space by the police directly, and therefore give limited indications as to situations where the competent authorities can ask a controller to disclose data, in particular with regards to the criteria listed under Annex II concerning the “appropriateness of methods”, which seems to concern the

⁶⁷ See Annex II page 8.

⁶⁸ See Annex II page 7.

⁶⁹ See Annex II page 8 – two Supreme Court decisions of December 24th, 1969 (1965 (A) No.1187) and April 15th, 2008 (2007 (A) No.839).

assessment of whether voluntary investigation is “appropriate” or reasonable in order to achieve the purpose of the investigation. The same can be said concerning the general criteria of “whether it can be considered reasonable in accordance with socially accepted conventions” to assess the legality of voluntary investigations. Furthermore, the National Police Agency, which is the federal authority in charge of all matters concerning the criminal police, issued instructions to the Prefectural Police on the “proper use if written inquiries in investigative matters”. Among others, the chief investigator must receive internal approval from a high-ranking official. The EDPB has no information if these instructions are binding. Nevertheless the EDPB states, that the use of this procedure has to be proportionate or necessary.

4.1.1.3.3 Rights and obligations of the controllers in the context of voluntary disclosure

148. In addition, it is for the controllers to consent to provide data (but there appears to be no obligation on their part to seek the consent of data subjects or to inform them), where these requests do not conflict with other legal obligations (such as confidentiality obligations). The report provided by the Commission seems to indicate that after a high rate of compliance, controllers have started taking into account data protection of their customers’ and thus have started answering less frequently to these requests.
149. It also remains unclear if controllers have any incentive to comply with the requests (for instance, if they have an advantage when complying, or if they are exempted from prosecution, etc). In particular, no mention is made of any principle such as the “non-self-incrimination principle”.
150. The EDPB would welcome additional information, if available, figures on the number and types of requests, as well as on the answers provided by the controllers requested. In the absence of case law and figures, the EDPB invites the Commission to monitor the efficiency and concrete application of this procedure in practice
151. However, the EDPB lacks case law and figures on this procedure to establish these elements. Consequently, the EDPB is not in a position to provide an assessment concerning the efficiency and concrete application of this procedure without further elements concerning the practice.

4.1.1.4 Conclusion on procedures for accessing data for law enforcement purposes

152. As a conclusion, the EDPB acknowledges that the principle according to which personal data can be compulsorily accessed by the competent authorities only when necessary and proportionate to the purpose, and on the basis of a warrant, corresponds to the main essential guarantees provided under EU and ECHR law. Following the findings above, the EDPB asks the Commission to monitor the scope of these measures, the scope of the voluntary disclosure procedure and the application of these principle by the Prefectural Police and by the Courts in the relevant case law and to monitor too, if the Japanese legal framework is providing the essential guarantees drawn by the CJEU on the basis of the Charter and the ECHR on the basis of the Convention.

4.1.2 Oversight in the field of criminal law

153. The draft adequacy decision as well as the Annex II present four types of oversights conducted on the police, ministries and public agencies.

4.1.2.1 Judicial oversight

4.1.2.1.1 In cases where electronic information is collected by compulsory means (search and seizure)

154. According to the draft adequacy decision, in all cases where electronic information is collected by compulsory means (search and seizure), the police has to obtain a prior court warrant. However, there

is an exception to this rule.⁷⁰ Indeed, article 220 (1) of the Code of Criminal Procedure allows a public prosecutor, its assistant or a judicial police official, when they are arresting a suspect to search or seize electronic information on the spot of the arrest. In this situation, there is a possibility for those information to be excluded as evidence by a judge.

155. The EDPB is mindful that similar exceptions also exist under EU law. It notes that there is not always a judicial control in cases where electronic information is collected by compulsory means, as it is stipulated in the draft adequacy decision. In this context, the EDPB recalls the jurisprudence of the ECHR on judicial a posteriori checks.⁷¹

4.1.2.1.2 In the case of requests for voluntary disclosure

156. According to the draft adequacy decision, in the case of the requests for voluntary disclosure, there is no ex ante control by a judge. In such case, the Prefectural Police operates under the supervision of the public prosecutor. The draft adequacy decision mentions articles 192 (1) and 246 on the mutual cooperation and coordination of the prosecutors, Prefectural Public Safety Commission and Judicial Police Officials and exchange of information between them. It also refers to article 193 (1) according to which public prosecutor may give necessary instruction to judicial police as well as setting standards for fair investigation. Finally, it mentions article 194 on the disciplinary actions against judicial police for not respecting the public prosecutors taken by the National or Prefectural Public Safety Commission.
157. The EDPB acknowledges the establishment of the previous measures and the oversight conducted by National and Prefectural Public Safety Commission on the judicial police (see below).

4.1.2.2 Oversight by the Public Safety Commissions of the police

158. According to the Annex II of the draft adequacy decision, two types of commissions are exerting an oversight of the police. Both aim at securing democratic management and political neutrality of the police administration.

4.1.2.2.1 Oversight conducted by the National Public Safety Commission

159. Annex II of the draft adequacy decision mentioned the oversight conducted by the National Public Safety Commission on the NPA. The Police Law gives a list of the duties of the Commission from which emanates its supervisory powers (see Article 5).
160. According to Article 4 of the Police Law, the National Public Safety Commission is established under the jurisdiction of the Prime Minister and is composed of a chairman and five members. Article 7 establishes some limitations to the appointment of the members of the Commission. The term of Office of Members of the Commission is five years and may be re-conducted one time only, as prescribed in Article 8. Furthermore, the Diet, appears to have a strong power over the appointment and the dismissal of the Commission's member which ensure the independence of the National Public Safety Commission.
161. Such legal provisions enhance the political neutrality of the National Public Safety Commission.

4.1.2.2.2 Oversight conducted by Prefectural Public Safety Commissions

162. The Prefectural Police is subject to the oversight of the Prefectural Public Safety Commissions established in each prefecture. According to Articles 2 and 36 (2) of the Police Law, the Prefectural Public Safety Commissions are responsible for "the protection of rights and freedom of an individual". Article 38 as well as Article 42 of the Police Law list the duties of the Prefectural Public Safety

⁷⁰ See Annex II.

⁷¹ ECHR, Modestou v. Greece, N° 51693/13.

Commissions. Those Commissions also aim at securing democratic management and political neutrality of the police administration as stated in Article 43 (2) by issuing to the Prefectural Police individual cases when they consider this necessary in the context of an inspection of the activities of the Prefectural Police or misconduct of its personnel.

163. However, it is unclear whether those Commissions have other powers than the inspection of police's behavior. The EDPB is wondering whether the term "misconduct" is including illegal access of data and, in such a case, whether those Commissions are able to order the deletion of data or not.
164. Regarding the neutrality and the independence of those Commissions, as stated in the draft adequacy decision⁷², Prefectural Public Safety Commissions are established under the jurisdiction of the prefectural governor who has to appoint members of the Commission with the consent of the prefectural assembly. Members of the Prefectural Public Safety Commission have a three years term and may be re-appointed up to two times. Article 39 of the Police Law enounced limitations concerning the appointment of the members. The draft adequacy decision also mentions the oversight of the Prefectural Police by local assembly, making reference of Article 100 of the Local Autonomy Act. However, this act was not provided to the EDPB⁷³.
165. Furthermore, according to Article 42 (2) and (3) of the Police Law, "No member of the Commission shall become concurrently a member of the assembly or the personnel in full-time service of local public entities or be engaged in part-time service prescribed in the provision of paragraph 1, Article 28 (5) of the Local Public Service Law.
166. According to the elements stated above and considering the collaboration between Prefectural Public Safety Commissions and National Public Safety Commission, the EDPB agrees with the draft adequacy decision and welcomes the neutrality and the independence of the members of the Prefectural Public Safety Commissions. The EDPB understands that Prefectural Safety Commissions only have a power to investigate police's behavior and do not have other supervisory powers, including the deletion of data collected by the prefectural police. Therefore, it appears that further clarification is needed as to whether the oversight conducted by Prefectural Public Safety Commissions is sufficient according the standards established under EU law.

4.1.2.2.3 Oversight conducted by the Diet

167. The draft adequacy decision⁷⁴ and the Annex II⁷⁵ are providing some information about the oversight conducted by the Diet in relation to the government, including with respect to the lawfulness of information collection of data by the police. Indeed, both mention the Article 62 of the Constitution according to which, the Diet may request the production of documents and the testimony of witnesses. Both are also mentioning legal provisions from the Diet Law, especially Article 104, concerning the powers of the Diet as well as Article 74 on the submission of written inquiries, which have to be answered by the Cabinet in writing within seven days as prescribed in Article 75. The draft adequacy decision also adds "The Diet's role in supervising the executive is supported by reporting obligations, for instance pursuant to Article 29 of the Wiretapping Act".
168. The EDPB acknowledges the implication of the Diet in the oversight of the government and the police regarding the lawfulness of data collection.

⁷² See draft adequacy decision p. 31.

⁷³ See draft adequacy decision p. 33.

⁷⁴ See draft adequacy decision p. 30.

⁷⁵ See Annex II, p. 12.

4.1.2.2.4 Oversight conducted by the executive

169. According to the Annex II of the draft adequacy, on the one hand, the Minister or Head of each ministry or agency has the authority of oversight and enforcement based on the APPIHAO⁷⁶. On the other hand, the Minister of Internal Affairs and Communications (MIC) has an investigative power concerning the enforcement of the APPIHAO by all other ministries, including the Minister of Justice for the Police as mentioned in the draft adequacy decision⁷⁷.
170. The Minister may request the head of an administrative organ to submit materials and explanations regarding the handling of personal information by the concerned administrative organ based on Article 50 of the APPIHAO. It may request a revision of the measures when it is suspected that a violation or inappropriate operation of the Act has occurred as well as issuing opinions concerning the handling of personal information by the concerned Administrative Organ according to Articles 50 and 51 of the APPIHAO.
171. The draft adequacy decision and the Annex II are also mentioning the establishment of 51 comprehensive information centres which are “ensuring the smooth implementation of this Act” according to Article 47 of the APPIHAO. The EDPB notes that the APPIHAO does not explain further the role and powers of those information centres but the draft adequacy decision provides some precisions.
172. Therefore, the EDPB welcomes the fact that there is an executive oversight on the respect of the APPIHAO on Ministries and administrative organs by the MIC.
173. As a conclusion, EU laws and the ECHR, in the jurisprudence of their respective Courts, are establishing standards and guarantees according to which the oversight has to be complete, neutral and independent. The EDPB notes that the PPC does not have supervisory powers in matters related to law enforcement. Furthermore, if the oversight conducted by the Diet, the National and Prefectural Safety Commission appears to be neutral and independent, further clarification is needed about the supervisory powers of the Prefectural Public Safety Commissions.

4.1.3 Redress in the field of criminal law

174. The draft adequacy decision, complemented by Annex II, presents several avenues through which individuals can bring their complaints, both before independent authorities and before judges.
175. These avenues and the core elements of these procedures stemming from the available documentation are presented here after, following a brief overview of the available rights to clarify what data subjects can expect from public authorities in the context of data processing in the field of criminal procedures.

4.1.3.1 Available rights of data subjects in the context of criminal procedures

176. In order to obtain redress, data subjects need to have rights under the law to be able to claim they were not respected. Therefore, the EDPB also assessed the available rights in the context of criminal procedures presented in the draft adequacy decision.

⁷⁶ See Annex II p. 10.

⁷⁷ See Annex II p. 11.

4.1.3.1.1 General limitations to the rights of data subjects under the APPIHAO

177. In its draft adequacy decision, the COM refers to and relies on general data protection principles which public authorities have to respect, once they have collected personal data. These principles are also further outlined in the Annex II so that the EDPB has decided to also comment on them.
178. Concerning available rights, the EDPB notes that, according to Annex II of the draft Adequacy decision, some of the general rights provided to data subjects in the context of data processed by Administrative organs, remain available also in the context of criminal investigations. However, additional limitations with regard to the collection and further handling of personal information in this context also follow from the APPIHAO itself.
179. These limitations, which also appear to apply both in the context of data collected on the basis of a warrant as well as on the basis of an enquiry sheet in the context of voluntary disclosure, raise questions concerning several aspects.
180. Concerning the principle of purpose limitation, although in principle administrative organs are required to specify the purpose for which they retain personal data, and shall not retain them beyond the scope necessary for the achievement of the purpose of use specified, they can change the purpose if it is “what can reasonably be considered as appropriately relevant for the original purpose”.
181. The APPIHAO also provides for the principle of non-disclosure, according to which an employee shall not disclose the acquired personal information to another person without a justifiable ground or use such information for an unjust purpose. However, no additional information is provided concerning the interpretation of what “justifiable ground” or “unjust purpose” could cover, so that further clarification would be necessary for the assessment.
182. Article 8(1) of the APPIHAO also lays down the prohibition to use or disclose data “except as otherwise provided by laws and regulations”. Nevertheless, although this provision is not in principle contrary to the level of protection afforded under EU law, the EDPB lacks additional elements concerning the extent to which any supervision or checks is exercised when disclosure is provided by laws or regulations. In addition, under Article 8(2), additional exceptions apply to this rule where “such exceptional disclosure is not likely to cause unjust harm to the rights and interests of the data subject or a third party”. Without any further elements on this point, this exception, which relies on the unclear notion of “unjust” harm, needs further clarification, if it is narrow enough.
183. Lastly, Article 9 of the APPIHAO provides for additional restrictions on the purpose or method of use or any other restrictions, to be imposed by the head of an administrative organ where retained personal information is provided to another person. As the notions of “any other necessary restrictions” and “provided to another person” are very broad, these additional restrictions to the rights of data subjects raise concerns without further clarifications on the scope of this provision.
184. While the EDPB is fully aware that access rights and other data protection principles are also limited in criminal proceedings under EU law, additional safeguards are provided when such limitations are foreseen, including in terms of supervision, oversight and redress. In the absence of sufficient case law on these limitations or additional elements to clarify the scope of these provisions, the EDPB is not in a position to assess whether these limitations to the rights of data subjects are limited to what would be considered strictly necessary and proportionate under EU law, and would thus be essentially equivalent to the rights provided to the EU data subjects.

4.1.3.1.2 Additional limitations to the rights of the APPIHAO deriving from the Code of Criminal Procedure and the Prefectural Police ordinances

185. The EDPB notes that although the APPIHAO seems to be applicable to all processing by administrative organs in Japan, some important limitations to the rights of data subjects derive from specific legislations. In particular, Article 53 (2) of the Code of Criminal Procedure⁷⁸ provides that “personal information recorded in documents relating to trials and seized articles” are excluded from the scope of application of the individual rights in Chapter IV of the APPIHAO. Concretely, the EDPB therefore understands that in the context of criminal procedures, data subjects do not benefit from the rights to information, access, rectification or erasure for personal data recorded in documents relating to trials and seized articles.
186. With regards to these limitations, the EDPB understands that they apply in the context of data collected on the basis of warrants, as well as in the context of data collected under the voluntary disclosure through enquiry sheets (see below). Indeed, the legal basis of the two procedures to access data (through a warrant and through an enquiry sheet) being provided in the code of criminal procedure, Article 53-2 of this code appears to apply to both types of collection. However, as Article 53-2 refers to the articles “seized” it could be clarified whether the limitations to the rights foreseen under this provision do apply also in the context of voluntary disclosure.
187. The EDPB regrets not to be provided with the ordinances of the Prefectural Police, which are said to be protecting personal information, rights and obligations equivalent to the APPIHAO. Given both the unclarities regarding the interpretation of the APPIHAO and the unavailability of the Prefectural Police ordinances, the EDPB wonders, if the granted rights to the individuals in this context, and the additional oversight and/or redress mechanisms are sufficient to compensate the absence of rights.

4.1.3.2 Redress through independent authorities redress

4.1.3.2.1 Administrative redress

188. The EDPB notes that the administrative organs collecting data, such as the Prefectural Police, are competent to deal with requests stemming from individuals concerning their – limited – rights with regards to their data collected as part of criminal investigations (see above concerning the rights available), which appear to include both the collection of data based on a warrant and on enquiry sheets. Concretely, these rights seem to be limited to general principles, such as the necessity of data retention, in connection with the purpose (see Article 3.1 APPIHAO), the purpose limitation principle (Article 4) or the accuracy of the data (Article 5), while individual rights such as the right to information, access, rectification or erasure are excluded for personal data recorded in documents relating to trials and seized articles⁷⁹. Although these organs cannot be considered as independent and therefore as providing independent redress or oversight, the EDPB welcomes this avenue. However, it stresses that complaints filed in this context remain limited to very few rights of the data subjects given the limitations of rights provided by the APPIHAO.
189. Furthermore, as “personal information recorded in documents relating to trials and seized articles” are excluded from the scope of application of the individual rights in Chapter IV of the APPIHAO pursuant to Articles 53-2 of the Code of Criminal Procedure, the possibilities to request access to personal information are also limited to the procedures foreseen under other provisions of this Code of Criminal Procedure. It seems that only victims, suspected or accused persons can act in this context, and still,

⁷⁸ Available here <http://www.japaneselawtranslation.go.jp/law/detail/?printID=&id=2283&re=02&vm=02> and quoted in Annex II of the draft adequacy decision, footnote 25.

⁷⁹ See supra concerning the limitations to APPIHAO and in particular see article 53-2 of the Code of Criminal Procedure (not provided but quoted in annex II of the draft adequacy decision, footnote 25).

depending on the stage of the criminal procedure. Therefore, the EDPB is concerned that no general right to access and/or rectify or delete information is available to data subjects under Japanese law in the context of criminal procedure, and that all redress avenues available imply to be either a victim (in which case the person would probably know that his/her data were collected) or a suspect or accused person, or the demonstration of a damage, while data subjects should also have the right to have access to their data and possibly to have their data rectified or deleted when they did not suffer any damage (yet possibly) and/or when they are neither a victim, a suspect or an accused person, but witnesses for instance.

[4.1.3.2.2 Administrative redress through the Prefectural Public Safety Commissions](#)

190. In addition, the Prefectural Public Safety Commissions appear to be competent to deal with complaints. Based on Article 79 of the Police law referred to in the draft adequacy decision, individuals can complain against any illegal or improper behaviour of an agent in the execution of his/her duties.
191. The EDPB seeks clarification whether any “illegal” processing of personal data qualifies for an “illegal or improper behaviour of an agent” and on the demonstration of a disadvantage which seems required from the data subject. Indeed, the notice issued by the NPA to the Police and Prefectural Public Safety Commissions on the proper handling of complaints regarding the execution of duties by police officers limit the complaints to concrete claims concerning “correction for any specific disadvantage that has been inflicted as the result of an illegal or inappropriate behaviour, or failure to take a necessary action, by a police officer in his/her execution of duty” and the possibility to “file grievance/discontent about inappropriate mode of duty execution by a police officer”. It is expressly clarified that “complaints on non-performance of a police officer concerning any matter that is not considered to fall under a police officer's duty, and also those expressing a general opinion or a proposal, not directly affecting the complaining party itself, shall be excluded”.
192. Concerning the procedural requirements to file a complaint, although they have to be filed in writing, the EDPB notes that assistance for writing the complaint is provided in this context under Japanese law, including for foreigners. In addition, the Japanese government seems to have also entrusted the PPC with the duty to provide assistance to EU data subjects to handle and resolve complaints in this field, which the EDPB welcomes. The EDPB underlines that in its understanding, in this context, the PPC will only act as a point of contact between the EU data subjects and the competent authorities in Japan.
193. The results of the Prefectural Public Safety Commission following a complaint shall not be noticed in cases listed in Article 79-2 of the Police Act, which includes the case where the current “resident of the complainant is unknown”. The EDPB acknowledges that the reference to the resident does not imply that in all cases EU data subjects would therefore be excluded from the notification of the results of their complaints on the ground they are not residing in Japan.

[4.1.3.2.3 Ad Hoc mechanism implying the PPC](#)

194. In view of the findings described above, The EDPB welcomes that the Japanese government and the EU Commission have agreed on an additional redress mechanism providing EU individuals with an additional avenue for redress in Japan through which individuals can also seek redress against unlawful or improper investigations by public authorities. The EDPB also notes and welcomes that the requests can be lodged with the PPC, rather than with another government official, thereby extending the scope of competence of the PPC to the area of law enforcement and national security.
195. The focus of the EDPB, when analysing the new mechanism, has been to understand the powers the PPC has in this context.

196. Even though the language is not entirely clear, the EDPB understands that the additional redress mechanism does not require “standing” in the meaning that the requestor is not required to show that her personal data is likely to have been subjected to surveillance by a Japanese authority. The EDPB would still like to request confirmation by the Commission.
197. In line with its assessment of the Ombudsperson mechanism, created under the Privacy Shield, the EDPB stresses the need for effective powers of the addressee of the request, in this case the PPC, in order to consider the redress mechanism as essentially equivalent to an effective remedy in the meaning of Art. 47 of the Charter on Fundamental Rights.
198. When explaining the redress mechanism, the Japanese government refers to Art. 6, 61 (ii) and 80 APPI and lays out these powers in Annex II. It is the understanding of the EDPB that the procedure as described in Annex II specifies or extends the powers of the PPC, as the language in Art. 6, 61 (ii) and 80 APPI is rather vague and general. To the extent Annex II specifies or extends the powers of the PPC, the EDPB would like to ask for clarification that the other agencies of the Japanese government are bound by them.
199. On the basis of the procedure in Annex II, the EDPB notes that the competent public authorities in Japan are required to cooperate with the PPC, “including by providing them with the necessary information and relevant material, so that the PPC can evaluate whether the collection or the subsequent use of personal information has taken place in compliance with the applicable rules”. For the assessment of the effectiveness of the system, it is thus important to refer again to the powers that those competent authorities have with which the PPC cooperates. It is the understanding of the EDPB that those powers would not be extended through the reassurances in Annex II.
200. The EDPB also notes that, if a violation of the rules has been identified, “the cooperation by the concerned public authorities with the PPC includes the obligation to remedy the violation”, which expressly includes the deletion of the data collected in violation of the applicable rules. The EDPB understands that the obligations of the competent authority stem from the “cooperation with the PPC”, rather than from a decision by the PPC.
201. Finally, the PPC will inform the requestor of the “outcome of the evaluation, including any corrective action taken where applicable.” In addition, the PPC will inform the requestor about the “possibility of seeking a confirmation of the outcome from the competent public authority and about the authority to which such a request for confirmation shall be made.”
202. In addition, the PPC has committed to assist the requestor with bringing further action under Japanese law, if the requestor is dissatisfied with the outcome of the procedure.
203. In light of the need to have an effective redress mechanism essentially equivalent to the EU standards, the EDPB nevertheless wonders if the PPC has any specific powers other than evaluating whether the collection or the subsequent use of personal information has taken place in compliance with the applicable rules and calling on the competent authorities to use their respective powers and to deal with complaints forwarded to them by the PPC. Should the PPC only act as a contact point for the EU individuals, the EDPB would consider this as insufficient to provide for an effective redress mechanism essentially equivalent to the EU standards. The EDPB thus calls on the Commission to provide clarifications on the points mentioned in this sub-chapter, in particular on whether and how the mechanism extends the obligations of competent authorities, how they are bound by it, and how the PPC can effectively ensure compliance and not only acting as a contact point for EU individuals.

4.1.3.3 Judicial redress

4.1.3.3.1 Quasi complaint mechanism

204. The so-called “quasi-complaint” procedure allows to act against compulsory collection of information based on a warrant to have an illegal seizure rescinded or altered.
205. This avenue implies the individual is aware of the data being seized. However, the EDPB understands that the procedure for the collection of data based on a warrant is not notified to the data subject. Equally, it understands that voluntary disclosure does not imply that companies requested have the obligation to inform the data subjects of requests received and complied with. Therefore, although it is stressed in the Annex II that “such a challenge can be brought without the individual having to wait for the conclusion of the case”, in practice, apart for warrants authorising wiretapping, for which it is indicated that the Law provides for a notification requirement⁸⁰, this avenue seems to be effectively available only once the data subject got aware of the collection through a case brought against her or him.

4.1.3.3.2 Injunctive relief

206. In addition, in order to obtain the deletion of data collected through a criminal procedure (the so-called “injunctive relief”), or to obtain compensation of damages, individuals can also bring civil actions before a judge.
207. As regards compensation, the EDPB notes that the procedure seems to be circumscribed to situations where a public officer in the course of his duties, unlawfully and with fault (intentionally or negligently) inflicted damage on the individual concerned. In the understanding of the EDPB, the damage appears to include moral damages. It is however not set out in further detail what needs to be demonstrated by the individual that he/she suffered a damage. The EDPB was not in a position to assess the case law concerning the award of compensation, and is therefore unable to assess whether this avenue provides for an effective remedy in case of damage.
208. With regards to the “injunctive relief”, the EDPB also notes that to file a request, the individual should first be aware that his/her data were collected and that they are still retained. Therefore, given the limited rights of information and access of individuals in the context of criminal investigations and procedures, the efficiency of the procedure appears to be rather limited too.

4.1.3.4 Overall assessment of the avenues for redress

209. Following the assessment of all the redress avenues open for individuals under Japanese law as well as to the EU data subjects before the PPC, the EDPB welcomes the *ad hoc* dispute resolution mechanism, involving the PPC. It has an added value for EU data subjects, in particular since it allows them to understand which avenues are available for them to obtain redress and/or compensation, as well as to present their requests according to the applicable procedural requirements under Japanese law. However, further clarifications are necessary, in particular on whether and how the mechanism extends the obligations of competent authorities, how they are bound by it, and how the PPC can effectively ensure compliance, in order to ensure that this new mechanism provides for effective redress.
210. This assessment shows that no redress mechanism in Japanese law appears to allow for access, rectification or deletion of data for data subjects who are not victims, suspects or accused in the context of a criminal procedure, for instance to remedy unlawful collection or retention of their data.

⁸⁰ Article 23 of the Wiretapping Act is mentioned page 33 of the draft adequacy decision, however the EDPB was not provided with this text and is therefore unable to assess to which extent this notification obligation applies and in which cases it might be limited.

It also shows that all redress and compensation mechanisms and procedures available under Japanese law for victims, suspects or accused person imply the knowledge of the collection of data, which appears to be limited in practice since limited rights of access and information are provided for them. In addition, further clarification appears necessary about the demonstration of an illegal behaviour on the part of the authorities, in particular whether such behaviour includes any illegal processing of personal data, or of a damage suffered by the individual.

211. Therefore, without further documentation and elements, the EDPB is concerned as to whether redress under Japanese law and under the draft adequacy decision is sufficiently effective compared to the standards in EU law.

4.2 Access for national security purposes

4.2.1 Scope of surveillance

212. In the draft adequacy decision, the chapter on “access and use by Japanese public authorities for national security purposes” is introduced by a general statement, in line with the reassurance provided by the Japanese government in Annex II, according to which no Japanese law would provide and thus permit “compulsory requests for information or “administrative wiretapping” outside criminal investigations”. As a conclusion, it is said that “on national security grounds information may only be obtained from an information source that can be freely accessed by anyone or by voluntary disclosure. This excludes any covert surveillance activities in this area. Business operators receiving a request for voluntary cooperation (in the form of disclosure of electronic information) are under no legal obligation to provide such information.”⁸¹
213. Within these limitations, four government entities are listed which have the power to collect electronic information held by Japanese business operators on national security grounds. With regard to the Ministry of Defence, as one of those four entities, it is said that it “only has authority to collect (electronic) information through voluntary disclosures”.⁸²
214. For its assessment of the general setup of data collection for the purpose of national security, the EDPB wishes to recall the first of the four so called “essential guarantees”, according to which “processing should be based on clear, precise and accessible rules”.⁸³ More specifically, the ECHR has been very clear that surveillance programs are only “in accordance with the law” if the surveillance measures “have some basis in domestic law”. The court has clarified that compatibility with the rule of law requires the law authorizing the measure must be accessible and foreseeable as to its effects. Referring to the risk of arbitrariness, the court has required “clear, detailed rules on secret surveillance measures”; “sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measure”.⁸⁴
215. For the application of these essential guarantees to the legal system of Japan, the EDPB is aware not only of the fact that, in matters of national security, states have a broad margin of appreciation, recognized by the European Court of Human Rights. Also, national security powers reflect the historical experiences nations make. The EDPB thus understands that, as emphasized by the Japanese

⁸¹ Adequacy decision, paragraph 151.

⁸² Adequacy decision, paragraph 153.

⁸³ WP29, WP 237: Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees).

⁸⁴ See e.g. Big Brother Watch and others v. the United Kingdom, paragraph 305.

government, after World War II, Japanese national intelligence agencies have been equipped with more limited powers than in other states.

216. In the reading of the EDPB, the draft adequacy decision, in line with the reassurance by the Japanese government, suggests that Japanese government entities do not run programs, which strategically monitor or broadly surveille (internet) communication. As said above, the Japanese government has given reassurance, in a letter signed by the Minister of Justice, that “on national security grounds information may only be obtained from an information source that can be freely accessed by anyone or by voluntary disclosure”.
217. As to the legal basis of the Ministry of Defence, the EDPB notes that the draft adequacy decision includes general information about its powers and quotes its mission “to conduct such affairs as related thereto in order to secure national peace and independence, and the safety of the nation”. However, the EDPB has not been provided with an English translation of the legal basis.
218. At the same time, the EDPB is aware of reports published in different media suggesting that surveillance programs are run by the Directorate for Signals Intelligence of Japan’s Ministry of Defense (MOD).⁸⁵ In the report, it is also claimed that the Japanese Ministry of Defense, while refusing to discuss specifics of the report, has “acknowledged that Japan has “offices throughout the country” that are intercepting communications” and that those “would be focused on military activities and “cyberthreats” and are “not collecting the general public’s information”. The latter statement (that the MOD does not collect information on the general public) is made part of the restatement by the Japanese government.
219. It stands that the Japanese government has restated, in a letter signed by the Minister of Justice, that the MOD does not collect information on the general public.
220. It is beyond the task of the EDPB to make a general assessment of the possible surveillance capabilities of the Japanese government. Those activities are only important for its assessment if they are relevant for the transfer of personal data between the EU and Japan. In this context, the EDPB would like to reaffirm its approach already adopted by its predecessor when asked to opine on the EU-U.S. Privacy Shield. When giving an opinion on the Privacy Shield, the WP29 included in its analysis the powers and limits of the U.S. to conduct surveillance of data “on its way” to the U.S.⁸⁶ Applying the same standard for the adequacy decision on Japan, the EDPB takes the view that information on the powers of Japanese authorities to surveille data “on its way” to Japan are relevant. Should these surveillance powers exist, also the decision in Big Brother Watch by the ECHR appears to suggest that such powers would have to be regulated in accordance with the standards established by the ECHR.
221. As a consequence, if interceptions were limited to the “assistance of military action”, they may well not be relevant for the assessment of the adequacy decision. It is thus the interest of the EDPB to receive clarifications on the surveillance measures by Japanese governmental entities. In this respect, such clarification would be welcome in order to determine whether data undergoing transfer under

⁸⁵ In May 2018, the online news publication “The Intercept” published a report titled “The untold story of Japan’s secret spy agency”.

⁸⁶ See WP255, EU-U.S. Privacy Shield –First annual joint review, adopted on 28 November 2017, p. 16: “WP29 is of the view that the analysis of the laws of the third-country for which adequacy is considered, should not be limited to the law and practice allowing for surveillance within that country’s physical borders, but should also include an analysis of the legal grounds in that third-country’s law which enable it to conduct surveillance outside its territory as far as EU data are concerned. As already underlined in its previous opinion, “it should be clear that the Privacy Shield Principles will apply from the moment the data transfer takes place, which means including as regards data “on its way” to that country.”

this adequacy framework could be the subject of access for national security purposes by the Japanese competent authorities in that field.

4.2.2 Voluntary disclosure in case of national security

222. The draft adequacy decision states that the four government entities only have the authority to collect (electronic) information by voluntary disclosure. According to the draft decision and Annex II, there are some limitations on statutory grounds, which means that the collection of data is limited to what is necessary for the execution of the tasks by the entities.
223. In the area of criminal law, as mentioned in the section about law enforcement, voluntary disclosure is only permissible as part of a criminal investigation, and thus presupposes a concrete suspicion of a crime that is already committed. Investigations in the area of national security differ from investigations in the area of law enforcement. The EDPB acknowledges that, according to Annex II, the central principles of “necessity for investigation” and “appropriateness of method” similarly apply in the area of national security and have to be complied with taking appropriate account of the specific circumstances of each case.⁸⁷ It regrets that the application is not further clarified, including by way of further reference to case law. Nevertheless the EDPB states, that the use of this procedure has to be proportionate or necessary.
224. According to the draft decision, when personal information has been collected (“obtained”), its handling is governed by the APPHAO except for the Prefectural Police.⁸⁸ Annex II states that the handling of personal information by the Prefectural Police is governed by prefectural ordinances that stipulate principles for the protection of personal information, rights and obligations equivalent to the APPHAO.⁸⁹ Because there are no English translations available for these ordinances, the EDPB is not in a position to assess whether the principles are equivalent to those of the APPHAO.
225. For the other remarks on voluntary disclosure, reference is made to the section on law enforcement.

4.2.3 Oversight

4.2.3.1 General Points

226. The four government entities empowered to collect electronic information held by Japanese business operators on national security grounds, are: (i) the Cabinet Intelligence & Research Office (CIRO); (ii) the Ministry of Defence ("MOD"); (iii) the police (both National Police Agency (NPA)⁹⁰ and Prefectural Police); and (iv) the Public Security Intelligence Agency ("PSIA").
227. According to the draft adequacy decision, these government entities are subject to several layers of oversight from three branches of the government⁹¹. The EDPB notes that there are oversight mechanism within the legislative branch (Japanese Diet) and the executive branch (Inspector General's Office of Legal Compliance (IGO), the Prefectural Public Safety Commissions and the Public Security Examination Commission). The EDPB stresses that the COM should clarify the judicial oversight (*ex-officio/guarantee C* of the WP 237; for redress, there is a separate chapter in the draft decision and an extra guarantee in the WP 237) of the above-mentioned government bodies, as it is unclear whether

⁸⁷ See Annex II, pp. 23.

⁸⁸ Adequacy decision, paragraph 118 and 157.

⁸⁹ See Annex II, pp. 3.

⁹⁰ However, according to the information received, the main role of the NPA is to coordinate investigations by the various Prefectural Police departments and its information collection activities are limited to exchanges with foreign authorities.

⁹¹ See Annex II, pp. 39.

there is such a judicial oversight in the area of collection of personal information for national security purposes without compulsory means.

4.2.3.2 *Oversight by the Japanese Diet*

228. The EDPB notes that the Japanese Diet may conduct investigations in relation to the activities of public authorities, therefore also for all of the aforementioned government entities. Furthermore, the diet may also request the production of documents and the testimony of witnesses (*Article 62 of the Japanese Constitution, Article 104 Diet Law*). The EDPB also remarks that according to *Articles 74 and 75 Diet Law*, Diet members may ask written questions to the Cabinet which may end in an answer from the Cabinet (*Article 75 Diet Law*). Finally, it is as well noted that there are specific reporting obligations for e.g. the Public Security Intelligence Agency (PSIA) (Article 36 SAPA/Art 31 ACO), by means of a yearly report to the Diet. Such a report was not provided to the EDPB.

4.2.3.3 *Oversight by the Inspector General's Office of Legal Compliance (IGO)*

229. The EDPB notes that there is an oversight body for the MOD, called IGO. The EDPB was not provided with the MOD Establishment Act (Act for the Establishment of the MOD), but only with the representations in Annex II to the draft decision. Pursuant to Annex II, the IGO is an independent office within the MOD, which is under the direct supervision of the Minister of Defense according to Article 29 of the MOD Establishment Act. The IGO has the powers of carrying out inspections of compliance with laws and regulations by officials of the MOD (« so called « Defense Inspections »), across the entire ministry including the Self-Defense Forces.
230. Pursuant to the Annex II, the IGO performs its duties independently from MOD's operational departments. The EDPB notes that the IGO is an *internal* oversight body.
231. Inspections lead to findings and, with the intention to ensure compliance, measures which are directly reported to the Minister of Defence. Based on the report of the IGO, the Minister of Defence may issue orders to implement the measures necessary to remedy the situation. The Deputy Vice minister of Defence is responsible for implementing these measures and must report to the Minister of Defence on the status of such an implementation.
232. Analysing Annex II, without being provided with the legal provisions (MOD Establishment Act) for this considerations, the EDPB welcomes the possibility of ordering necessary compliance measures to remedy the situation. However, the EDPB raises doubts regarding the independence of the IGO, as it is an office within the MOD and is under direct supervision of the Minister of Defence pursuant to Annex II (according to the *WP 237 « functional independence is not by itself sufficient to protect that supervisory authority from all external influence »*).
233. In alignment to the case law of the ECHR and the *WP 237* respectively following the considerations of Annex II, the Inspector General can request for reports from the concerned office (documents, sites, explanations). Clarification as to whether the offices concerned are obliged to follow these requests or not and whether the requested documents include closed materials, like the *WP 237* mentions or not, appear necessary to the EDPB.
234. Although the EDPB welcomes that very senior legal experts (former Superintending Prosecutor) head the IGO, clarification about the manner of appointment of this supervisory body appears necessary.

4.2.3.4 *Oversight by Public Security Examination Commission*

235. According to Annex II (page 25), PSIA carries out regular and special inspections on the operations of its individual bureaus and offices (Public Security Intelligence Bureau, Public Security Intelligence Offices and Sub Offices, etc). For the purposes of the regular inspection, an Assistant Director General

and/or a Director are designated as inspectors. Such inspections should also concern the management of personal information.

236. Pursuant to recital 163 of the draft decision the *Public Security Examination* Commission operates as an independent ex ante oversight body for the PSIA, with regards to issues of the ACO⁹² and SAPA⁹³. The EDPB welcomes that.
237. Although the website of the Japanese Ministry of Justice provides some information⁹⁴, the EDPB is not in the position to carefully further assess the independency of the Public Security Examination Commission since it was not provided with the Act of the establishment of the Public Security Examination Commission⁹⁵ and the Rules of the Public Security Examination Commission⁹⁶.

4.2.3.5 Oversight by National Public Safety Commission, Prefectural Public Safety Commissions and the APPIHAO (executive)

238. See 3.1.2.2.1 (National Public Safety Commission), 3.1.2.2.2. (Prefectural Public Safety Commissions) and 3.1.2.2.4. (Executive).

4.2.3.6 Oversight by PPC

239. The EDPB invites the COM to either mention in Recital 164 that the PPC is not an oversight body for the aforementioned government entities and that it is only competent for the redress of the individuals or to move the passage in recital 164 about the PPC to the section « individual redress ».

4.2.4 Redress mechanism

240. For the analysis of the newly negotiated redress mechanism, reference is made to the section on law enforcement.
241. In addition, it is noteworthy that the Japanese law provides for a specific individual redress avenue available in the area of national security. It is the understanding of the EDPB that all individuals, including EU individuals, may generally request disclosure, correction (including deletion) or suspension of use from the administrative organs, also if those are processed for national security purposes. In case such a request is “rejected on the grounds that the concerned information is considered non-disclosable”, an appeal for review may be lodged, and the “Information Disclosure and Personal Information Protection Review Board” has to be consulted. The Board is composed of members appointed by the Prime Minister with the consent of both Houses, equipped with investigative powers, and concludes with a written report for the concerned individual, which is not

⁹² Act on the Control of Organizations Which Have Committed Acts of Indiscriminate Mass Murder (Act No. 147 of December 7, 1999).

⁹³ Subversive Activities Prevention Act(Act No. 240 of July 21, 1952).

⁹⁴ See <http://www.moj.go.jp/ENGLISH/MEOM/meom-01.html> (September 2018): *the extra-ministerial organ ”is composed of a chairperson and six members. They are selected from among persons of good character who are capable of making a fair judgment on the control of organizations and those who have ample knowledge and experience of both law and society. They are appointed by the Prime Minister and must be approved by both houses of the Diet. With regard to the application of the previously mentioned laws (SAPA/ACO), the members perform their duties quite independently, free from any direction or supervision of the Prime Minister or the Minister of Justice.”*

⁹⁵ http://www.japaneselawtranslation.go.jp/law/detail_main?re=&vm=2&id=613 (September 2018).

⁹⁶ Article 28 ACO.

legally binding, but almost always followed.⁹⁷ According to Annex II, there were only two out of 2000 cases, where an administrative authority took a decision that differed from the Board's conclusion.⁹⁸

242. It appears to follow from the explanation provided that the review is not available, if the information can be "disclosed" but the individual is dissatisfied with the outcome. The EDPB acknowledges this avenue for redress, but would like to seek further clarification on the latter aspect, which would significantly limit its scope.

For the European Data Protection Board
The Chair
(Andrea Jelinek)

⁹⁷ Annex II, p. 25, 26. Act for Establishment of the Information Disclosure and Personal Information Protection Review Board, Art. 4, 9, 11.

⁹⁸ Annex II, footnote 35.

Opinion of the Board (Art. 64)



Opinion 4/2019

**on the draft Administrative Arrangement for the transfer of
personal data between European Economic Area (“EEA”)
Financial Supervisory Authorities and non-EEA Financial
Supervisory Authorities**

Adopted on 12 February 2019

Table of contents

1	Summary of the Facts.....	4
2	Assessment.....	4
3	Conclusions/Recommendations.....	7
4	Final remarks	8

The European Data Protection Board

Having regard to Article 63, Article 64 (2), (3) - (8) and Article 46 (3), (b) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018, as amended on 23 November 2018.

Whereas:

(1) With reference to Article 46 (1), (3) (b) and 46 (4) GDPR, in the absence of a decision pursuant to Article 45 (3), a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. Subject to authorisation from the competent supervisory authority ("competent SA"), the appropriate safeguards may also be provided for, in particular, by provisions inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

(2) Taking into account the specific characteristics of the administrative arrangements provided for by Article 46 (3) (b)¹, which may vary considerably, each case should be addressed individually and is without prejudice to the assessment of any other administrative arrangement.

(3) The EDPB ensures pursuant to Article 70 (1) of the GDPR the consistent application of Regulation 2016/679 throughout the European Economic Area. Under Article 64 (2), the consistency mechanism may be triggered by a supervisory authority, the EDPB Chair or the Commission for any matter of general application or producing effects in more than one Member State. The EDPB shall issue an opinion on the matter submitted to it provided that it has not already issued an opinion on the same matter.

(4) The opinion of the EDPB shall be adopted pursuant to Article 64 (3) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

(5) Pursuant to Article 65 (1) (c) GDPR where a competent SA does not follow the opinion of the EDPB issued under Article 64, any supervisory authority concerned or the Commission may communicate the matter to the EDPB and it shall adopt a binding decision.

¹ See also recital 108 GDPR

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. Following several rounds of discussions , the European Securities and Markets Authority (ESMA), acting as facilitator for EEA financial supervisory authorities (NCAs) and in its own capacity, and the International Organisation of Securities Commission (IOSCO) have submitted by official letter the attached draft Administrative Arrangement (hereinafter draft AA) according to Article 46 (3) (b) GDPR to frame the transfers of personal data from EEA NCAs (and ESMA itself) to their non-EEA counterparts. This draft AA was communicated to the Chair of the EDPB on 2 January 2019.
2. Following the submission, the Chair of the EDPB has requested the Board for an opinion pursuant to Article 64(2) GDPR. The decision on the completeness of the file was taken on 15 January 2019.

2 ASSESSMENT

3. The draft AA may be used by all market regulators in the EEA and submitted to the competent SAs for authorisation. As a result, the matter is producing effects in more than one Member States within the meaning of Article 64(2) GDPR.
4. The draft AA is necessary to ensure efficient international cooperation between these authorities, acting in their capacity as public authorities, regulators and/or supervisors of securities and/or derivatives markets, in order to “safeguard investors or customers, and to foster integrity and confidence in the securities and derivatives markets” in accordance with their mandates as defined by applicable laws.
5. In assessing the provisions contained in this specific draft AA, the EDPB has taken into account a number of specific elements for the assessment of possible risks posed by the transfers of personal data including the type of personal data subject to the AA and the objectives pursued.
6. The draft AA which can be found in its entirety in the attachment includes the following guarantees:
 - **Definitions of GDPR concepts and data subject rights:** Section II of the AA contains the relevant definitions necessary to determine the scope of the AA and its consistent application. Among them there are some definitions of key concepts and rights of the European data protection legal framework such as “personal data”, “processing”, “personal data breach”, “right of access”, “right of erasure” which are in line with the definitions contained in the GDPR.
 - **Principle of purpose limitation and prohibition of any further use:** Section III (1) of the AA works on the premise that Authorities have specific responsibilities and regulatory mandates, which include protecting investors or customers and fostering integrity and confidence in securities and/or derivatives markets. According to the principle of purpose limitation, the transfers can therefore only take place in the framework of such mandates and

responsibilities, namely if necessary to support their institutional tasks and the receiving Authority will not be allowed to further process the personal data in a manner that is incompatible with these purposes.

- **Principle of data quality and proportionality:** According to Section III.2 of the AA the transferring Authority will only transfer accurate and up to date personal data that are adequate, relevant and limited to what is necessary for the purposes for which they are transferred and further processed. Each Authority will inform the other if it becomes aware that transferred personal data is incorrect. Having regard to the purposes for which the personal data have been transferred and further processed, each Authority will supplement, erase, block, correct or otherwise rectify the personal data, as appropriate.
- **Principle of transparency:** A general notice to data subjects will be provided by each Authority in relation to the processing carried out, including the transfer, the type of entities to which data may be transferred, the rights available to them under the applicable legal requirements, including how to exercise those rights and information about any applicable delay or restrictions on the exercise of such rights and the contact details for submitting a dispute or claim. This notice will be provided by each Authority on its website where it will be published along with this Arrangement. Furthermore, individual notice will be provided to data subjects by EEA Authorities in accordance with the GDPR and, in the case of ESMA, in accordance with Regulation 2018/1725.
- **Principle of data retention:** As provided by Section III.7 of the AA the Authorities will retain personal data for no longer than is necessary for the purpose for which the data are processed in compliance with the applicable laws.
- **Security and confidentiality measures:** Section III.4 envisages that each receiving Authority will have in place appropriate technical and organizational measures to protect personal data that are transferred to it against accidental or unlawful access, destruction, loss, alteration, or unauthorized disclosure, including, for example, marking information as personal data and restricting who has access to personal data.

The AA also envisages that in the case where a receiving Authority becomes aware of a personal data breach, it will inform the transferring Authority as soon as possible and use reasonable and appropriate means to remedy the personal data breach and minimize the potential adverse effects.

- **Safeguards relating to data subject rights:** Section III (5) of the AA provides for safeguards relating to data subject rights. Data subjects can obtain confirmation of whether their data have been transferred to another financial supervisory Authority outside the EEA (TCA). Data subjects will also be provided with access to their personal data upon request. In addition, data subjects may request directly to the concerned NCA or TCA that their data are rectified, erased, restricted or blocked. Information regarding these safeguards are to be provided on the NCA/TCA website. Any restriction to these rights has to be provided by law and is allowed only to the extent and for as long as this is necessary to protect confidentiality or for important objectives of general public interest which when the transferring Authority is an EEA NCA, has to be recognized by the Member State of this NCA (including, for instance, to prevent prejudice or harm to supervisory/enforcement functions).
- **Restrictions on onward transfers:** Onward transfers to a third party in another country who is not an Authority participating in the AA and is not covered by an adequacy decision from the

European Commission will only take place with the prior written consent of the transferring Authority, and if the third party provides appropriate assurances that are consistent with the safeguards in the AA.

The same safeguards are envisaged for cases of sharing of personal data with a third party in the same country of the receiving Authority unless, in exceptional cases, such third party cannot provide the aforementioned assurances. In this case, the transfer may take place only if the sharing is “for important reasons of public interest”. When the transferring Authority is an EEA NCA, this public interest has to be recognized by the Member State of this NCA.

Personal data may be shared with a third party in the same country of the receiving Authority (such as public bodies, courts, self-regulatory organizations and participants in enforcement proceedings) without consent from the transferring Authority, or assurances only in two cases:

(i) If the purpose for which the personal data are shared and then used is consistent with the purpose for which the data were initially transferred or with the general framework of the use stated in the original specific request from the receiving Authority, and the sharing is necessary to fulfil the mandate and responsibilities of the receiving Authority and/or the third party.

(ii) When the sharing of personal data follows a legally enforceable demand or is required by law. The receiving Authority will notify the transferring Authority prior to the sharing and include information about the data requested, the requesting body and the legal basis for sharing. The receiving Authority will use its best efforts to limit the sharing of personal data received under this Arrangement, in particular through the assertion of all applicable legal exemptions and privileges.

- **Redress:** Section III (8) of the AA provides for a redress mechanism. This mechanism is there to ensure the right to obtain redress and, where appropriate, to receive compensation. In cases where non-compliance of the AA occurs, including where data subject rights are violated, redress can be exercised before a competent body (e.g. court). Redress before such a competent body will be in accordance with the applicable legal requirements, ensuring that the rights of the data subject related to the principles and safeguards provided for under the AA can be effectively enforced. The transferring Authority will be informed about any dispute or claim and the authorities on both sides will use best efforts to settle the dispute or claim amicably. In the event the matter cannot be resolved in this way, other methods will be used to resolve the dispute, including non-binding mediation or dispute resolution mechanisms. If the transferring Authority is of the view that a receiving Authority has not acted consistent with the safeguards set out in the AA, e.g. as it has not followed the decision of the non-binding mediation or alternative dispute resolution mechanism, it will suspend any transfers under the AA to the receiving Authority until the issue is satisfactorily resolved. Moreover, the “assessment group” (as well as all other Authorities) will be notified and can, in case it determines that there has been a “demonstrated change in the willingness or ability of [the receiving Authority] to act consistent with the [AA]”, recommend that the receiving Authority’s participation in the AA be discontinued. In order to enable data subjects to exercise their right of redress, the AA will be made publicly available.
- **Oversight mechanism:** Section IV of the AA provides for an external oversight mechanism ensuring the implementation of the safeguards of the AA. This oversight mechanism consists of a combination of periodic reviews conducted by the “assessment group” and by each NCA/TCA internally. The combination of the external and internal oversight as well as the

possible consequences following a negative review – which may include a recommendation to suspend an Authority's participation in the AA – provides for a satisfactory level of protection.

7. The EDPB welcomes the efforts made for this multilateral AA which includes a number of important data protection safeguards. In order to make sure that these safeguards continue to ensure an appropriate level of data protection when data are transferred to a third country under this AA, taking into account the unique nature of such non - binding agreements, the EDPB underlines the following:
8. Each competent SA will monitor the AA and its practical application especially in relation to sections III (5), (6), (8) and IV relating to data subject rights, onward transfers, redress and oversight mechanisms to ensure that data subjects are provided with effective and enforceable data subject rights, appropriate redress and that compliance with the AA is effectively supervised.
9. Each competent SA shall only authorise this AA as a suitable data protection safeguard with a view to the cross-border data transfer, conditional to full compliance by the signatories with all the clauses of the AA.
10. Each competent SA, will suspend the relevant data flows carried out by the NCA in its Member State pursuant to the authorization, if the AA no longer provides for appropriate safeguards in the meaning of the GDPR.

3 CONCLUSIONS/RECOMMENDATIONS

11. Taking into account the above and the commitments the NCAs, ESMA and their non-EEA counterparts will undertake by signing this AA in order to have "*in place appropriate safeguards for the processing of such personal data in the exercise of their respective regulatory mandates and responsibilities*" and to "*act consistent with this Arrangement*", the EDPB considers that the AA ensures appropriate safeguards when personal data will be transferred on the basis of this AA to public bodies in third countries not covered by a European Commission adequacy decision.
12. Consistent with the preamble of the AA, acknowledging the importance of regular dialogue between the EEA NCAs and their competent SAs, or the European Data Protection Supervisor ("EDPS") in the case of ESMA, and in order to allow the competent SAs to carry out their task of monitoring and enforcing the application of the GDPR in accordance with Article 57 (1) (a) of the GDPR, the authorisation adopted by the competent SA should envisage that each signatory EEA NCA or ESMA shall inform the respective competent SA of any suspension of transfers of personal data based on Sections III (8) and IV of the AA, as well as of any revision or discontinuation of participation to the AA based on Section V.
13. In addition, the EDPB recalls that, in line with the accountability principle, each NCA and ESMA will need to keep records of information to facilitate the monitoring task of the SAs. This information should in any case be made available upon request from the competent SA. Each SA may also, in its authorisation, request to receive this information from NCAs or ESMA on an annual basis without any prior request. This information should include elements on the number of data subject requests and claims received by data subjects at EU level, details on the cases not resolved through the envisaged dispute resolution mechanisms as well as on respective findings and actions of the "Assessment Group" following the periodic reviews including actions with regards to the sharing of personal data

under Section 6.2.3 of the AA. Information should also be recorded on the notifications received by NCAs on the sharing of information to a third party by the TCA following a legally enforceable demand or required by law.

4 FINAL REMARKS

14. This opinion will be made public pursuant to Article 64 (5) (b) of the GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

EU - U.S. Privacy Shield - Second Annual Joint Review

Adopted on 22 January 2019

Table of contents

1	Executive summary	4
1.1	Introduction.....	4
1.2	On the commercial aspects of the Privacy Shield	4
1.3	On the access by public authorities to data transferred to the U.S. under the Privacy Shield	6
1.4	Conclusion	7
2	Introduction.....	8
3	On the commercial aspects of the Privacy Shield	9
3.1	Guidance for the companies adhering to the Privacy Shield	9
3.2	Clear and easily available information for EU individuals	10
3.3	Self-(Re)Certification Process and Cooperation between U.S. authorities in the Privacy Shield mechanism	10
3.4	Oversight and supervision of compliance with the Principles – Activities of the DoC.....	12
3.5	Oversight and supervision of compliance with the Principles – Activities of the FTC	13
3.6	Independent Recourse Mechanisms.....	13
3.7	HR Data.....	14
3.8	Automated-decision making/Profiling	14
4	On the derogations to the Privacy Shield to allow access to data for Law Enforcement and National Security purposes	16
4.1	Introduction.....	16
4.2	Collection of data (under section 702 and under EO 12333).....	16
4.2.1	Collection of data for national security purposes under Section 702.....	16
4.2.2	Collection of data for national security purposes under Executive Order 12333	17
4.3	Oversight	17
4.4	Redress for EU individuals.....	18
4.5	Ombudsperson mechanism	19
4.6	Access to data for law enforcement purposes.....	20
5	Conclusion	20
	ANNEX TO THE EDPB REPORT ON THE SECOND EU-US PRIVACY SHIELD ANNUAL JOINT REVIEW ...	22
	General Information.....	22
1	On commercial aspects	22
1.1	Self-Certification Process and Cooperation between U.S. authorities in the Privacy Shield Program.....	22
1.2	Oversight and supervision of compliance with the principles - Activities by the DoC.....	23
1.3	Oversight and supervision of compliance with the principles - Activities by the FTC.....	24

1.4	Oversight and supervision of compliance with the principles - Activities by the DoT	25
1.5	Guidance for the companies adhering to the Privacy Shield	25
1.6	IRM	25
1.7	Arbitral Panel.....	25
1.8	Automated Decision Making	25
1.9	HR Data.....	26
2	On government access to personal data: relevant developments in the U.S. legal framework and trends	27
2.1	Reauthorisation of 702 FISA.....	27
2.2	PPD-28	27
2.3	The Ombudsperson mechanism and the EU individual complaint handling body	27
2.4	PCLOB	28
2.5	Inspector General (IG) of the ODNI	28
2.6	Redress	28
2.7	Additional information on access to data by law enforcement authorities	29

The European Data Protection Board

Having regard to Article 4 and Recitals 145 to 149 of the Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (“EU - U.S. Privacy Shield),

HAS ADOPTED THE FOLLOWING REPORT:

1 EXECUTIVE SUMMARY

1.1 Introduction

1. According to the EU-U.S. Privacy Shield adequacy decision (“Privacy Shield”)¹ adopted on 12 July 2016, **seven representatives of the EDPB participated in the second joint review conducted by the European Commission, on October 18 and 19 of 2018** in Brussels to assess the robustness of its adequacy decision and its practical implementation.
2. Based on the concerns elaborated in the previous opinions of the WP29, in particular opinion 1/2016, and in its report following the first joint review, the EDPB focused on the assessment of both the **commercial aspects** of the Privacy Shield and on the **government access to personal data transferred from the EU for the purposes of Law Enforcement and National Security, including the legal remedies available to EU citizens**. The EDPB assessed once again whether these concerns have been addressed and also whether the safeguards provided under the EU-U.S. Privacy Shield are workable and effective.
3. The European Commission published its report of the second joint review on December 19, 2018.
4. **The EDPB’s main findings concerning this second joint annual review**, stemming both from written submissions and from oral contributions are hereby presented in this report.

1.2 On the commercial aspects of the Privacy Shield

5. The second annual review showed that **many of the WP 29’s findings of the first annual review regarding the commercial aspects have been taken into account by the US authorities**. The EDPB acknowledges that on the commercial aspects significant progress has been made especially with regards to the following aspects.
6. **The DoC has adapted the initial certification process** in a way that the inconsistencies between the Privacy Shield List and the representations made by the organizations regarding their participation in the Privacy Shield program on their websites are now avoided as far as the initial certification process is concerned.
7. **The DoC as well as the FTC have started to also take ex officio oversight and enforcement actions as regards the compliance of Privacy Shield certified organizations** with the requirements under the Privacy Shield.

¹ Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ L 207, 1.8.2016, p.1.

8. The DoC has issued further guidance for the EU individuals in order to facilitate their understanding of the Privacy Shield and the exercise of their rights. The DoC has also started to issue further guidance for the U.S. Businesses in order to clarify the requirements of the Privacy Shield. The EDPB still expects this guidance will provide the necessary clarifications to facilitate the proper application, and where necessary will be adjusted.
9. However, one of the main concerns already expressed by the WP29 remains a certain lack of oversight in substance. Indeed, the checks performed by the DoC are principally focused on formal aspects. The enforcement actions by the FTC could not be fully assessed during the review, since the FTC was not able to share substantial information on the subject matter of the new ex officio enforcement actions taken. This lack of substantial checks thus remains a concern of the EDPB as, even taking into account discretionary and limited investigations by the FTC, a majority of companies' compliance with the substance of the Privacy Shield's principles remains unchecked. The Privacy Shield presents in its Annex 1 "the clarification that Privacy Shield organizations must limit personal information to the information that is relevant for the purposes of processing" as an enhancement of the Privacy Shield. This is only one example for many substantial requirements set out by the Privacy Shield whose correct application has to be ascertained through sufficient oversight and enforcement action by the competent U.S. authorities.
10. Another issue where the EDPB sees further need to work on concern the area of onward transfers. Since onward transfers possibly lead to transfers of data outside of the jurisdiction of U.S. and EU authorities with possibly no data protection provided by law it is of utmost importance that the competent US Authorities closely monitor the practical implementation of the Privacy Shield's "Accountability for the Onward Transfers Principle". As a first step, for example the DoC could make use of its right to ask organizations to produce the contracts they have put in place with third countries' partners in order to assess whether those provide the necessary safeguards and to discover if any further guidance or other action by the DoC or the FTC is needed.
11. Another area that requires further attention is the application of the Privacy Shield requirements regarding HR Data. While the EU Supervisory authorities remain available to exchange with the US Authorities, the discussions on this issue will have to continue between the European Commission and the US Authorities given the different possible readings of the wording of the Privacy Shield. In parallel, the Commission is still called upon to address this issue and clarify the text in order to avoid that possible different interpretations do not lead to gaps in the protection of EU data subjects.
12. Also, the re-certification process needs to be further refined. The situation of outdated listings leads to avoidable confusion that should be addressed also in the interest of concerned Privacy Shield certified organizations.
13. Last but not least, the EDPB recalls the remaining issues with respect to certain elements of the commercial part of the Privacy Shield adequacy decision as already raised in the WP 29's Opinion 01/2016 in particular regarding the absence or the limitation to the rights of the data subjects (i.e. right to object, right to access, right to be informed for HR processing), the absence of key definitions, the lack of guarantees on transfers for regulatory purpose in the field of medical context, the lack of specific rules on automated decision making and the overly broad exemption for publicly available information. Those remain valid.

1.3 On the access by public authorities to data transferred to the U.S. under the Privacy Shield

14. The EDPB **welcomes the appointments of three new members of the Privacy and Civil Liberties Oversight Board (PCLOB), including its Chair, enabling it to reach the quorum.** It hopes that the two remaining positions will also be filled, which are important to respect the requirement concerning the bipartisanship of the members. The PCLOB is thus in a position again to prepare and issue reports.
15. The EDPB also welcomes the fact that the US authorities have published the report on Presidential Policy Directive 28 (PPD-28), in a redacted form, which mainly clarifies that the PPD-28 is applied by all agencies of the Intelligence Community, and it acknowledges the efforts made by the U.S. government by publishing a number of important documents, for example, decisions by the Foreign Intelligence Surveillance Court (FISA Court), in part by declassification, and the setting up of a new website.
16. Despite these developments, **some of the main points of concern, already expressed by the WP29 in this area in its previous report, still have to be fully resolved.**
17. More specifically, the **collection and access of personal data for national security purposes** under both Section 702 of FISA and Executive Order 12333 still remains an important issue for the EDPB, **especially with regards to massive and indiscriminate access** (on this issue, see in particular the statement of the WP29 on the decision of the European Commission on the EU-U.S. Privacy Shield of [26 July 2016](#)²).
18. In this respect, **the EDPB can only encourage the PCLOB to issue further reports**, on PPD-28 to follow up on the first report in order to provide additional elements as to how the safeguards of PPD-28 are applied, as well as a follow-up report on Section 702 FISA. The EDPB recalls that the WP29 considered a report on Section 702 important for assessing whether the collection of data under section 702 is not indiscriminate and access is not conducted on a generalized basis under the UPSTREAM program, and for assessing the necessity and proportionality of the definition of “targets”, the tasking of selectors under **section 702** (including in the context of the **UPSTREAM program**), as well as the concrete process of application of selectors in the context of the UPSTREAM program to clarify whether massive access to data occurs in this context.
19. **The EDPB regrets that the reauthorization of Section 702 FISA did not lead to the introduction of any new guarantees for EU individuals.** The EDPB recalls that, in its report following the first annual Joint Review in 2017, the WP29 considered that instead of generally authorizing surveillance programs, more specific safeguards would be needed, e.g. for precise targeting to determine whether an individual or a group can be a target of surveillance and for stricter scrutiny of individual targets by an independent authority ex-ante.
20. Concerning the application of **Executive Order 12 333** to EU data transferred to the U.S., the EDPB would welcome if the PCLOB finalized and issued its awaited report on EO 12 333 to provide information on the concrete operation of this Executive Order and on its necessity and proportionality.
21. The redress by EU citizens before U.S. courts is still to be effectively guaranteed due to the problematic admissibility threshold of the **“standing requirement”**. Therefore, the EDPB will continue to follow closely the evolution of the case law.

² https://ec.europa.eu/justice/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf

22. Hence, the independence of the Ombudsperson remains a key element, as this institution is designed to compensate the uncertainty in seeking effective redress before the court, if not the lack thereof. In any case, a permanent Ombudsperson **is still to be appointed**.
23. The exact powers of the Ombudsperson also need to be clarified through the **declassification of internal procedures** concerning the interactions between the Ombudsperson and the other elements of the intelligence community or oversight bodies. Based on the information provided so far, the EDPB is of the view that the powers of the Ombudsperson to remedy non-compliance vis-à-vis the intelligence authorities are still not sufficient in the light of Article 47 EU Charter of Fundamental Rights, and also underlines that the Ombudsperson is not in a position to bring a matter before the court.
24. Finally, regarding the **access to data for law enforcement purposes**, the EDPB underlines its remaining concerns on the available effective remedies for individuals in cases where the personal data processed by companies are accessed by law enforcement authorities.

[1.4 Conclusion](#)

25. The EDPB **welcomes the efforts made by the U.S. authorities and the Commission to implement the Privacy Shield, especially actions undertaken to adapt the initial certification process, start ex officio oversight and enforcement actions**, as well as the efforts made by the U.S Government by publishing a number of important documents and **the appointment of a new Chair as well as of two new members of the PCLOB**, meaning that the PCLOB has reached the required quorum for its functioning. However, the EDPB still has a number of significant concerns that need to be addressed by both the Commission and the U.S. authorities.
26. **The absence of substantial checks remains a concern of the EDPB. Other areas that require further attention are the application of the Privacy Shield requirements regarding onward transfers, HR Data and processors, as well as the recertification process.** In addition, the EDPB recalls the **remaining issues** with respect to certain elements of the commercial part of the Privacy Shield adequacy decision as already raised in the WP 29's Opinion 01/2016.
27. As regards the **collection of data by public authorities, the EDPB can only encourage the PCLOB to issue further reports**, including on PPD-28 to follow up on the first report in order to provide additional elements as to how the safeguards of PPD-28 are applied, on Section 702 FISA, and Executive Order 12333.
28. **On the Ombudsperson mechanism, the EDPB is still awaiting the appointment of a permanent independent Ombudsperson.** Given the elements provided, **the EDPB is not in a position to conclude that the Ombudsperson is vested with sufficient powers to access information and to remedy non-compliance, and it can thus not state that the Ombudsperson can be considered an “effective remedy before a tribunal” in the meaning of Art. 47 of the EU Charter of Fundamental Rights.**
29. Finally, the EDPB recalls that the **same concerns will be addressed by the European Court of Justice in cases that are already pending before the Court**.

2 INTRODUCTION

30. On 6 October 2015³, the European Court of Justice invalidated the Safe Harbor adequacy decision after having recalled the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the large number of persons whose fundamental rights are liable to be infringed where personal data is transferred to a third country not ensuring an adequate level of protection. Soon after, the Commission started negotiations for a new adequacy decision and presented a draft adequacy decision with its annexes.
31. On the 13 April 2016, the Working Party 29 issued an opinion⁴ on the draft new adequacy decision aiming at replacing the invalidated Safe Harbor. On the same day, the WP29 also issued a working document⁵ on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees).
32. On 30 May 2016, the European Data Protection Supervisor also issued an Opinion on the draft adequacy decision⁶.
33. On 12 July 2016, the European Commission adopted the EU-U.S. Privacy Shield adequacy decision⁷ ("Privacy Shield"). The Privacy Shield entrusts the Commission with the task to assess the findings of the adequacy decision, including on the basis of the factual information collected in the context of an Annual Joint Review⁸. Important concerns on both the commercial aspects and aspects relating to government access to personal data transferred under the Privacy Shield for the purposes of Law Enforcement and National Security had then to be addressed and further assessed in the context of the Joint Review.
34. As also foreseen in recital 147, "*participation in this meeting will be open for EU DPAs and representatives of the Article 29 Working Party*".
35. The WP 29 also issued a report following the first Joint Review of the Privacy Shield in November 2017⁹.
36. The second Joint Review of the Privacy Shield took place on the 18 and 19 October 2018 in Brussels. In addition to the Chair of the EDPB who gave an introductory speech, seven representatives of the EDPB, a Commissioner as well as experts at staff level, were designated to be part of the Review Team ("the Review Team") that accompanied the Commission during this two-day meeting with U.S. authorities and companies.

³ Case C-362/14

⁴ WP 238 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf

⁵ WP 237 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf

⁶ EDPS Opinion 4/2016 of 30 May 2016: https://edps.europa.eu/sites/edp/files/publication/16-05-30_privacy_shield_en.pdf

⁷ Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ L 207, 1.8.2016, p.1.

⁸ See recitals 145-149 and Article 4(4) of the decision.

⁹ WP 255: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48782

37. In advance to the Joint Review, the Commission sent questionnaires to US companies adhering to the Privacy Shield and NGOs, as well as a detailed agenda to organize the discussions with the US authorities and stakeholders during the Joint Review itself. The EDPB sent contributions to take part to the elaboration of these documents.
38. The new factual elements presented by the US authorities and companies participating in the Joint Review, stemming both from written submissions, as well as from oral contributions during the Joint Review itself, are presented in annex to this document. They were presented at the EDPB Plenary on 16 November.

3 ON THE COMMERCIAL ASPECTS OF THE PRIVACY SHIELD

3.1 Guidance for the companies adhering to the Privacy Shield

39. The EU-U.S. Privacy Shield is an adequacy decision that was designed to frame transfers of personal data outside the protections provided under GDPR to ensure the level of protection of natural persons guaranteed by GDPR is not undermined in the absence of a general law in the US providing for an essentially equivalent level of protection of personal data. It is of utmost importance that there is a common understanding of the text to ensure the application in the receiving State will correspond to the requirements for such transfers as set out under EU data protection law. It has to be ensured that this text is interpreted correctly and that organizations and individuals on both sides of the Atlantic are “on the same page” as regards their duties and rights under the Privacy Shield.
40. Thus, in the report of the first annual review the WP 29 emphasized the need for clear guidance on the application of the Privacy Shield principles. In the second year of operation of the framework and following informal consultation of members of the ITS at working level, the DoC has issued **guidance in the form of FAQs on the Accountability for Onward Transfer Principle¹⁰ and the notion of Processor**¹¹ and published it on its website.
41. The EDPB welcomes the issuance of these guiding documents that have been also highly demanded by participating organizations. This guidance should lead to the clarifications necessary to facilitate the proper application of the Privacy Shield Principles. In order to achieve this goal, the guidance concerning processors may further specify the application of the principles when it comes to processors (“agents”)¹².
42. Regarding the usability of the European Commission’s Standard contractual clauses in the context of onward transfers further work is required since the available clauses are designed only for transfers

¹⁰ <https://www.privacyshield.gov/article?id=Onward-Transfer-Principle-FAQs> (last accessed on 18 December 2018)

¹¹ <https://www.privacyshield.gov/article?id=Processing-FAQs> (last accessed on 18 December 2018)

¹² that the guidance could for example further elaborate on the following details: Notice to be provided by processors needs to be in line with the contract in place between the processor and the controller; that access to data and a Choice mechanism could be provided to the individual directly by the processor provided however that the controller has in the first place authorized the processor to do so; and that for a processor compliance with the Data Integrity and Purpose Limitation principle requires it to process the data only in accordance with the instructions from the controller and on the other hand to implement the appropriate measures as instructed by the controller to assist the later in complying with the data integrity principle.

from EU territory. In this context the EDPB calls upon the European Commission to also address this issue in the course of aligning the SCC with GDPR.

43. The EDPB regards the issuance of further guidance as a good start and expects that in the future there will be more guidance as to other key elements such as for example the **Choice Principle**, (on when and how a data subject can opt out from the processing of his/her data for a new purpose), and with respect to the **application of the Notice Principle** (more specifically on the timing for certified organizations to give notice to individuals). In addition, a **clarification of the scope of the right of access** could be helpful to prevent misunderstandings. In its last report worries regarding the possibly very narrowly interpreted duty to grant the right of access only to data that is “stored” by an organization voiced by the WP 29 remains valid.

3.2 Clear and easily available information for EU individuals

44. The WP 29 had found that to complement the specific information provided in concrete cases by the companies themselves, the US authorities should strive to offer **more information in an accessible and easily understandable form to the individuals regarding their rights and available recourses and remedies**.
45. The Privacy Shield website already had a specific section named “EU and Swiss individuals” containing subsections “My rights under Privacy Shield” and “Privacy Shield participants list”¹³ where individuals were informed about their rights. The various possibilities to lodge complaints were also explained and partly supported by direct links. After the first annual review and as a response to the WP 29s suggestions the DoC added a one-page document to their website that gives individuals an overview¹⁴ of the program with a strong focus on the individual’s rights and how they can be exercised. The EDPB acknowledges the efforts made by the DoC to provide further guidance for EU individuals on the Privacy Shield website. It remains to be seen if the Information given to the EU individuals both by the EU Supervisory Authorities and the DoC lead to the effect that more individuals are able to exercise their rights regarding the Privacy Shield properly.

3.3 Self-(Re)Certification Process and Cooperation between U.S. authorities in the Privacy Shield mechanism

46. Also in the certification process, the EDPB notes improvements:
47. The DoC reviews all self-certifications (both for first time applicants and for recertification submissions) and checks:
 1. Registration with an Independent recourse mechanism (IRM) company
 2. Payment of Annex I Arbitral Fund Contribution
 3. Compliance with Privacy Shield supplemental principle 6 (on access to personal information)
 4. Completion and consistency of certification information

¹³ See: <https://www.privacyshield.gov/Individuals-in-Europe> (last accessed on 27 November 2018)

¹⁴ See: <https://www.privacyshield.gov/servlet/FileDownload?file=015t000000QJdq> (last accessed on 14 December 2018)

- 5. Privacy notices (the existence of all 13 elements required by the Privacy Shield is checked also in the organizations Privacy Policy)
- 48. In order to prevent organizations from naming non-U.S subsidiaries as entities covered by their certification the DoC has produced more internal guidance for the review of applications regarding the identification of foreign entities.
- 49. Also, the DoC asks the organizations for more precise links provided for the Privacy Shield listing so individuals can more easily exercise their rights and for more than one point of contact within the organization to make sure messages from the DoC are received. The DoC also checks the applications for inconsistencies between the privacy policy and the certification (For example HR/NON HR).
- 50. The DoC has not finalized 100 first-time certifications and 30 re-certifications because the requirements set out by the Privacy Shield were not fulfilled. This appears to be an indication that the decision made by the DoC whether or not to list an organization on the Privacy Shield website is – as far as the checks go - not a rubber stamp exercise.
- 51. However, on the basis of the information given by the US authorities during the joint review, so far those checks do not go into the substance of the principles. The DoC for example does not check if the data transferred to an organization in the US acting as a controller is necessary and proportionate to the purpose, arguing that the Privacy Shield does not provide for checks with this level of detail. This absence of substantial checks remains a concern for the EDPB on the general question of sufficient oversight regarding the substance of the Privacy Shield principles.
- 52. As regards criticism on the procedure, which used to require US organizations to publish their Privacy Policy (with references to the Privacy Shield) before the checks of the DoC were finalized and the organization was put on the list of Privacy Shield active participants, the DoC has changed its procedure. The DoC now prohibits a first-time applicant from making public representations about participation until the PS Team approves its certification and instead requires an applicant to submit a draft privacy policy for review. It also directs an applicant to remove any premature references of their participation in the Privacy Shield program from their website.
- 53. As a result, **the concerns of the WP 29 regarding the inconsistencies between the Privacy Shield List and the representations made by the organizations on their websites seem to have now been resolved as far as the initial certification process is concerned.**
- 54. **Regarding the re-certification process**, the second annual review revealed that due to the established procedures there are cases where the due date displayed on the Privacy Shield List is already passed while the organization still is listed as an active participant. This occurs when an organization has submitted their recertification but the process is not finalized before the due date. This leads to confusion.
- 55. As long as the organizations still publicly commit to apply the Privacy Shield Principles this might not lead to a gap in the protection of individuals. **However the EDPB asks the DoC to explore what can be done to avoid this situation** (especially what can be done to guarantee that there is no gap in the protection of individuals) **and in the meantime to add some explanation for concerned individuals and EU based organizations using the Privacy Shield as a transfer tool so the situation is sufficiently clear to individuals and also organizations within the EU that would like to transfer personal data to a Privacy Shield certified organization and therefore check the validity of the certification on the Privacy Shield List.**

3.4 Oversight and supervision of compliance with the Principles – Activities of the DoC

56. In last year's report the WP 29 criticized that the **oversight of the commercial aspects of the Privacy shield mainly relied on the third party companies providing Independent Recourse Mechanisms (IRMs)** and that the **implementation** of the Privacy Shield framework **lacked sufficient oversight and supervision of compliance in practice**. Because the Privacy Shield is a program based on self-certification, it is of utmost importance that U.S. authorities involved in the administration of the Privacy Shield devote sufficient resources at oversight and enforcement activities. The WP 29 considered that the **performance of compliance reviews** of organizations having self-certified to the Privacy Shield is a key element for the effective functioning of the framework and that **ex-officio investigations have to be conducted both by the DoC and the FTC/DoT** to ensure that self-certified organizations concretely implement the requirements of the Privacy Shield.
57. This year's review showed that the U.S. authorities (namely DoC and FTC) have made significant efforts to address this concern:
- On a quarterly basis the DoC conducts "false claims reviews" in order to identify organizations that have started but not finished an initial or re-certification or that did not submit their annual re-certification at all.
 - The identified organizations receive a certified letter from the DoC, warning them of potential referrals to the FTC or DoT if they do not fulfil outstanding requirements or withdraw properly from the program. The DoC informs the FTC/DoT of its intent to send those letters. The organizations have 30 days to respond to the letter. The DoC compiles a list of those organizations that fail to take action and respond to the letter. This procedure has led to 100 referrals from the DoC to the FTC, 56 of those referral were made in the second year of the Privacy Shield program. DoC and FTC/DoT cooperate throughout the whole process. Simultaneously with the referral an organization is (at least temporarily) removed from the "active" Privacy Shield List.
 - As foreseen in the Privacy Shield text, the DoC also performs random web searches for false claims of participation in the program. Those web-searches have only led to few cases that were referred to the FTC.
 - The DoC has performed a sweep of 100 randomly chosen organizations. The focus of the sweep was the accessibility of the Privacy Policy, the responsiveness of the organization and the availability of the IRM. The DoC sent more in-depth compliance questionnaires to 21 organizations that showed minor or more significant peculiarities (for example: No response from the designated point of contact; the Privacy policy was no longer accessible online; Missing references to one or more elements of the notice principle). The organizations must respond within 30 days. If the response is not satisfactory, the organizations – similar to the procedure described above – receive a certified warning letter requiring the organization to indicate within a 30 day period how it has addressed the concerns. If those are not resolved within the 30 days the organization is moved to the "inactive" list and the case is being referred to the FTC or DoT.
 - The DoC has also designated 1 person to follow the media and to do keyword searches to identify possible breaches of the Privacy Shield commitments.

- The DoC also performs regular checks for broken links to the privacy policy on the Privacy Shield list.
58. **The EDPB welcomes all these steps taken by the DoC to ensure formal compliance with the Principles of the Privacy Shield. They are a good starting point; however, so far these checks remain focused on the formalities to be complied rather than on the substance.**
59. Further to monitoring concrete compliance with all principles of the framework, one of the areas that would need particular attention in this context remains the area of onward transfers. So far the DoC has not made use of its right to request a copy of the relevant privacy provisions of organizations contracts with their agents. Since onward transfers possibly lead to transfers of data outside of the jurisdiction of U.S. and EU authorities with possibly no data protection provided by law it is of utmost importance to closely monitor the practical implementation of the Accountability for the Onward Transfers Principle.

[3.5 Oversight and supervision of compliance with the Principles – Activities of the FTC](#)

60. Since last year's review the FTC also increased their activities regarding the enforcement of the Privacy Shield.
61. In the Division of Privacy and Identity Protection, Bureau of Consumer Protection there are 40 lawyers almost exclusively working only on privacy. They are supported by for example technical experts.
62. This year the FTC has brought 5 new Privacy Shield cases: 2 against organizations that did not complete their certification and 3 cases where the certification has lapsed. In most of those cases, the organization failed to verify the deletion, return or continued application of the Privacy Shield Principles to personal data transferred under the Privacy Shield.
63. The FTC investigates Privacy Shield-related referrals (about around 100 referrals, 8 of them being public) but in most cases by the time these referrals arrive to the FTC they have been solved in the meantime so many cases fall out.
64. As an experiment, the FTC has started to send out Civil Investigation Demands (CIDs) proactively to monitor compliance with the Privacy Shield Principles. The FTC could not provide more details on the selected targets or topics of this exercise. In general the FTC has a broad latitude to do sweeps. There is no need for the FTC to demonstrate that it has a reasonable suspicion. The objective is rather to identify where it is profitable to spend the resources.
65. **The EDPB welcomes the ex officio activity to proactively monitor compliance with the Privacy Shield Principles undertaken by the FTC. It nevertheless regrets that the FTC was unable to share any more detail on its approach as this leaves the EDPB unable to have a clear insight on the concrete activities and cases, and therefore to be in a position to assess how and to what extent the FTC ensures compliance monitoring with the substance of the Privacy Shield's principles.**

[3.6 Independent Recourse Mechanisms](#)

66. In order to make the reports provided by the various companies providing IRM services on an annual basis more useful the DoC gave out guidance to the IRM services in order to harmonize their reports. This guidance also highlights the possible conflicts of interest within companies providing both ex officio compliance and IRM services to the same organization and asks to describe the measures taken

to avoid such conflict of interests in the annual report. **The EDPB expects to see improved and comparable reports provided by the IRM services in the next annual review, that also explain how possible conflicts of interests are precluded.**

3.7 HR Data

67. As already stated by the WP 29 in last year's report, the notion of HR data in the context of the Privacy Shield is interpreted differently within the EU and by the US authorities. Although the DoC initiated the producing of guidance regarding the processing of HR data, including through informal consultation of members of the WP 29 on working level in this regard, the work on this guidance was not successful due to the absence of convergence on the definition of the notion of HR data. This year's review thus focused less on the definition of HR data but rather on the consequences, the different definitions within the EU and by US authorities may lead to. On the EU side, the concern is that additional protections granted by the Privacy Shield for employment data (opt-in to marketing purposes rather than opt out) would not and could not be enforced by any U.S or EU authority. The EDPB recalls that in its understanding, HR data should be protected in the same way whether they are processed by the employer or by a processor, including concerning the choice and purpose limitation principles. While the EU Supervisory authorities remain available to exchange with the US Authorities, the discussions on this issue will have to continue between the European Commission and the US Authorities given the different possible readings of the wording of the Privacy Shield. **In parallel, the Commission is still called upon to address this issue and clarify the text in order to avoid that possible different interpretations do not lead to gaps in the protection of employees in the European Union.**

3.8 Automated-decision making/Profiling

68. In last year's report, the WP29 **called upon the Commission to contemplate the possibility to provide for specific rules concerning automated decision making** to provide sufficient safeguards including the right to know the logic involved and to request reconsideration on a non-automated basis, especially after having explored the extent of the practical relevance of automated decision making processes by Privacy Shield certified companies if the analysis generates an actual need for additional safeguards.
69. As part of the second review the COM presented the main elements of a study¹⁵ commissioned to an independent contractor regarding the existence of automated decision-making on the basis of personal data that has been transferred from the EU to Privacy Shield certified companies in the US. While the authors of the study highlight a series of challenges for conducting this work (limited availability of experts on the topic and reservations to take part in interviews, limited relevance of answers in certain cases, opacity characterizing the data industry on such practices notably), the main conclusion that can be drawn from the study is that **automated decisions (in the narrow GDPR definition of decisions having legal effects on individuals) are not taken on the basis of data transferred from the EU.**
70. According to the study, such decisions are more likely to take place in "EU customer facing" situations (i.e. where the US company directly targets EU customers).

¹⁵ See: https://ec.europa.eu/info/sites/info/files/independent_study_on_automated_decision-making.pdf (last accessed on 19 December 2018)

71. **However, the study at the same time underlines that this is a fast developing area which still has to be closely monitored in the future.**
72. Some private companies (such as Workday and Salesforce) confirmed that they are offering services to their customers (EU businesses) which can be AI-based and potentially conduct some automated decisions¹⁶. However, these companies insisted that in any case they always act as data processors under the instructions of data controllers based in the EU.
73. According to the study, several credit-reporting agencies have self-certified under Privacy Shield (notably Experian, one of the three big major reporting companies in the US). The FTC has general enforcement jurisdiction over these agencies, in cooperation with the US Consumer financial bureau, which has supervisory authority over credit-reporting agencies (such companies have different products - some of these products may fall under the US Fair Credit Reporting Act). The Consumer financial bureau would pass on cases to the FTC so the same principles apply to such companies and if they are misrepresented the FTC would enforce them.
74. The FTC publicly announced that they are investigating the Equifax data breach case¹⁷.
75. The FTC also presented the RealPage company case¹⁸, which is offering background screening services by conducting criminal checks and automated decisions making by using weak accuracy verification methods¹⁹. The FTC asked the company to put in place a better, reasonable procedure to ensure first names' accuracy. This case led to a 3 million dollars fine settlement²⁰.
76. There was no other significant new developments as regards Automated Decision Making to take note of.
77. **The EDPB invites the European Commission to monitor cases related to automated decision making and profiling and to contemplate the possibility to foresee specific rules concerning automated decision making to provide sufficient safeguards, including the right to know the logic involved and to request reconsideration on a non-automated basis where an actual need for additional safeguards is identified.**

¹⁶ See for example the "Prism Analytics" tool offered by Workday which allows companies to "bring data in at scale from any source and prepare, analyze and securely share it with[in the] organization" (see <https://www.workday.com/en-us/applications/prism-analytics.html>) and the AI-based predictive marketing tool "Einstein" proposed by Salesforce (see: <https://www.salesforce.com/products/einstein/overview/>).

¹⁷ See: <https://www.ftc.gov/equifax-data-breach> (last accessed on 28 November 2018).

¹⁸ See: <https://www.ftc.gov/news-events/press-releases/2018/10/texas-company-will-pay-3-million-settle-ftc-charges-it-failed> (last accessed on 28 November 2018).

¹⁹ According to the abovementioned US FTC's press release: "(...) *RealPage compiled screening reports through an automated system that used the applicant's first name, middle name when available, last name, and date of birth when searching for criminal records. Its matching criteria only required an exact match of an applicant's last name along with a non-exact match of a first name, middle name, or date of birth, the FTC alleges. For example, if RealPage searched an applicant named Anthony Jones born on October 15, 1967, it would deem a match if it found a criminal record for Antony Jones 10/15/67, Antonio Jones 10/15/67 and Antoinette Jones 10/15/67.*"

²⁰ See: <https://www.ftc.gov/enforcement/cases-proceedings/152-3059/realpage-inc>

4 ON THE DEROGATIONS TO THE PRIVACY SHIELD TO ALLOW ACCESS TO DATA FOR LAW ENFORCEMENT AND NATIONAL SECURITY PURPOSES

4.1 Introduction

78. **The EDPB welcomes that the U.S. government has continued to publish a number of important documents**, e.g. decisions by the Foreign Intelligence Surveillance Court²¹ (FISA Court), in part by declassification, as well as through the new website set up. These publications and declassifications continue to demonstrate the efforts by the U.S. government and of the U.S. legislator to become more **transparent** about the use of surveillance powers. In addition, these documents help to better understand how the various surveillance programs are operated, including their safeguards. The additional explanations and answers provided during the two Joint Reviews also helped the EDPB to get a clearer understanding of these programs and safeguards and of their concrete impact on the level of data protection in place.
79. Nevertheless, some of the main points of concern that the WP29 expressed in its previous opinions, in the area of access to data transferred under the Privacy Shield for national security or law enforcement purposes, have not been fully resolved. These **main concerns are related to the collection of data, to oversight, to judicial redress and finally, to the Ombudsperson mechanism. This calls for a more detailed analysis.**

4.2 Collection of data (under section 702 and under EO 12333)

4.2.1 Collection of data for national security purposes under Section 702

80. In its Schrems judgment²², the CJEU recalled that the “*protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary*”²³ and ruled that “*legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter*”²⁴.
81. **The previous concerns expressed by the WP29 remain relevant**, as the legal framework has not significantly changed on any of the aspects concerning the collection of data from the perspective of EU individuals. Therefore the EDPB recalls the concerns expressed previously by the WP29 in this respect.
82. **The EDPB also regrets that in the context of the re-authorization of section 702 FISA last year, the US legislator did not take the opportunity to introduce additional safeguards.**
83. The EDPB thus maintains its call for further independent assessment on the necessity and proportionality of the definition of “targets” and of the tasking of selectors under section 702 (including in the context of the UPSTREAM program), as well as the concrete process of application of

²¹ U.S. federal court established and authorized under the Foreign Intelligence Surveillance Act of 1978 (FISA)

²² Case C-362/14, 5 October 2015

²³ See recital 92, See also cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger, recital 52.

²⁴ See recital 94.

selectors in the context of the UPSTREAM program to clarify whether massive and indiscriminate access to personal data of non-U.S. persons takes place.

84. **The EDPB would welcome if the Privacy and Civil Liberties Oversight Board (PCLOB), as an independent oversight agency with a quorum (see infra), should now be in a position to prepare and issue an updated report on Section 702, building on the report issued in 2014.**

4.2.2 Collection of data for national security purposes under Executive Order 12333

85. **In the context of the second Joint Review, given the disagreements between the EDPB, on the one hand, and the European Commission and the US authorities on the other, as to the relevance of Executive Order 12333 for the adequacy decision, the application of legislation was not further discussed.**
86. The EDPB recalls the WP29 long-standing position that the analysis of the laws of the third-country for which adequacy is considered, should not be limited to the law and practice allowing for surveillance within that country's physical borders, but should also include an analysis of the legal grounds in that third country's law which allow it to conduct surveillance outside its territory as far as EU data are concerned. Necessary limitations to governmental access to data should extend to personal data "on its way" to the country, for which adequacy is recognized. This is why the WP29 analysed the Executive Order 12333 and the Presidential Policy Directive 28 (PPD-28), which is all the more important in this context as it provides for the only safeguards and limits to the collection and use of data collected outside the U.S. as the limitations of FISA or other more specific U.S. law do not apply. During the Joint Review, the U.S. authorities underlined again that Executive Order 12333 could not be used as a basis for collection of data inside the U.S. territory and that they consider that collection of data under this Executive Order falls outside the scope of the Privacy Shield.
87. The WP29 welcomed the adoption of PPD-28. The current U.S. government confirmed its commitment during the Joint Review to comply with the rules set therein, which the EDPB welcomes. Indeed, the PPD-28 provides limitations to the collection of data, as the signal intelligence activities have to be as "tailored as feasible". The EDPB notes that the recently published report by the PCLOB on PPD-28 confirms that it has been transposed into the internal policies of the relevant authorities. **However, neither the report nor the Second Joint Review provided substantial new information concerning the application of this text**, especially on the interpretation of the six purposes allowing for the use of data foreseen in this text, or on additional elements as to the amount of personal data collected in order to allow for a validation of the commitments and the assurances provided. Here again, given the uncertainty and unforeseeability of how EO 12333 is applied, the EDPB would welcome if the PCLOB finished and issued its awaited report on EO 12333 to provide information on the concrete operation of this Executive order and on its necessity and proportionality.
88. In addition, a more detailed follow-up report on how the PPD-28 applies to the different surveillance programs would be welcome to provide additional elements on these aspects.

4.3 Oversight

89. The EDPB recalls that comprehensive **oversight of all surveillance programs** is crucial, as the CJEU and the ECtHR have also emphasized in many judgments.
90. **Additional presentations were made during the second Joint Review by the different institutions of which the oversight structure consists. Although these elements brought few new elements, they**

confirmed the understanding of the EDPB, of the architecture and functioning of the Inspector General community.

91. Already during the first annual Joint Review, the WP29 was presented with the oversight activities of several entities and considers that a **comprehensive internal oversight structure**, independent from the Intelligence Community, is in place, including the Privacy and Civil Liberty officers, the oversight of the Department of Justice, and Inspector Generals, amongst others.
92. As expressed in the previous opinions of WP29, the EDPB is aware of the complex and multi-layered oversight structure established in the U.S. in order to ensure that personal data is collected and processed in accordance with U.S. law. As underlined in the previous report of the WP29, the EDPB remains of the view that the offices of **the Inspector Generals**, institutions rarely known in most EU Member States, provide valuable checks on the US government's agencies.
93. **The EDPB welcomes the appointment of a new Chair as well as of two new members of the PCLOB. This means that the PCLOB has reached the required quorum for its functioning just before the second Joint Review, although the remaining vacant positions and the requirement for this organ to be bipartisan are yet to be fulfilled.** As emphasized before, the EDPB considers the **PCLOB**, whose recommendations have been an important contribution to reforms in the U.S. and whose reports have been a particularly helpful source to understand the functioning of the various programs, as an independent body, to be an essential element of the oversight structure.

4.4 Redress for EU individuals

94. In its Schrems ruling, the CJEU stressed the importance to have a right to an effective remedy before a tribunal²⁵. A third-country can only be considered as providing an adequate level of protection in accordance with the GDPR, where EU individuals have access to an independent and impartial redress body, including in surveillance matters.
95. **As the U.S. government informed during this year's Joint Review that the legal framework remained unchanged and no significant new case law concerning these matters needed to be considered, the EDPB recalls its position and the relevant criteria to take into account when assessing the level of adequacy are still those stemming from the jurisprudence of the highest courts in Europe, meaning the CJEU and ECtHR.**
96. As underlined in the previous report of the WP29, while the APA and FISA appear to provide limited grounds for an EU individual to challenge surveillance in U.S. courts, the principal problem appears to concern the "**standing requirement**".
97. Under the procedural requirements as currently interpreted by the U.S. courts, it appears to be difficult and uncertain that an EU individual could satisfy the procedural requirement of standing when bringing a suit against a surveillance measure on the basis of section 702 FISA or EO 12333. The EDPB will therefore continue to follow closely the evolution of these cases as they could provide additional guarantees concerning the effectiveness of judicial redress offered before U.S. courts. However, as was confirmed during the Joint Review, the interpretation of the notion of "standing" in surveillance matters is evolving with cases still pending²⁶.

²⁵ See paragraph 95

²⁶ See in particular cases ACLU v. Clapper, and Wikimedia v. NSA

4.5 Ombudsperson mechanism

98. **The most significant element in the context of the second Joint Review was the nomination of a new acting Ombudsperson, Mrs Manisha Singh, on 28 September 2018.**
99. Since the effective remedy before an independent tribunal is of such importance in the jurisprudence of the European courts, the WP29 welcomed the establishment of an **Ombudsperson** mechanism as a new redress mechanism in its previous opinion. It underlined that this may constitute a significant improvement for EU individuals' rights with regards to U.S. intelligence activities. The Ombudsperson mechanism complements the possibilities of redress, or more critically, it might be argued that it is meant to compensate for the uncertainty or unlikeliness to seek effective redress before a U.S. court in surveillance matters. In addition, as the PPD-28 does not create rights, it was confirmed that the individual cannot go to court based on an alleged violation of the PPD-28. Thus, the only way for EU individuals to ask for a verification that the relevant authorities have complied with the requirements of this instrument is to ask the Ombudsperson to refer the matter to the competent Inspector General to check the internal policies of these authorities.
100. With Art. 47 of the Charter of Fundamental Rights in mind, the threshold for independence and impartiality required in a redress mechanism such as the Ombudsperson is high. Having analysed the jurisprudence of the ECtHR in particular, the WP29 took into account the powers of the Ombudsperson, in particular the powers to access information as well as to remedy non-compliance. When assessing the Ombudsperson mechanism in its opinion and its report of last year, the WP29 suggested that the appointment of a high-ranking official in the Department of State as the Ombudsperson, who can be dismissed at any time without notice, is problematic.
101. During the first and the second Joint Review, as well as before the EDPB Plenary in July 2018, the previous and new acting Ombudspersons and the U.S. government explained in some detail the important work done in order to ensure that requests would be handled lawfully and efficiently. The two acting Ombudspersons also stressed that they needed to be convinced of the findings before responding to the request and Mrs Singh also underlined during the second Joint Review that she could escalate the issue should she be unconvinced by the outcome presented to her following the assessment of a request. While the EDPB still has no reason whatsoever to doubt the integrity of the new (acting) Ombudsperson, **it recalls that a permanent Ombudsperson should be appointed as soon as possible as well as its expectation to learn more about the powers that the Ombudsperson has vis-à-vis the Intelligence Community.** This information however remains partial. The procedures governing the access to relevant information by the Ombudsperson and governing the interactions of the Ombudsperson with the other members of the Intelligence Community, including the oversight bodies, remain partially classified. The EDPB acknowledges that the acting Ombudsperson explained how a theoretical case would be handled during the Joint Review.
102. Based on the available information, the EDPB still doubts that the powers to remedy non-compliance vis-à-vis the intelligence authorities are sufficient, as the "power" of the Ombudsperson seems to be limited to decide not to confirm compliance towards the petitioner. In the understanding of the EDPB, the (acting) Ombudsperson is not vested with powers, which courts or other similarly independent bodies would usually be granted to fulfil their role. Therefore, the EDPB remains unable to hold that the Ombudsperson is vested with adequate powers to effectively exercise its duty. In addition, it was confirmed during the Joint Review that the decisions of the Ombudsperson cannot be brought to court.

103. The EDPB recalls the lack of judicial review of the decisions of the Ombudsperson and consequently the impossibility to obtain remedies where the Ombudsperson will not provide any answer. **As a conclusion, the EDPB is not be in a position to conclude that the Ombudsperson is vested with sufficient powers to access information and to remedy non-compliance, and it can thus not state that the Ombudsperson can be considered an “effective remedy before a tribunal” in the meaning of Art. 47 of the Charter of Fundamental Rights.**²⁷

4.6 Access to data for law enforcement purposes

104. As regards **access to data for law enforcement purposes**, the EDPB continues to note that the procedural safeguards inherent to the criminal procedure seem to imply that data are accessed for a specific purpose and that individuals are notified that their data have been accessed within the framework of criminal proceedings, in the context of which they can have access to judicial redress. However, it recalls its concerns as regards effective remedies available to individuals in cases where the data processed by companies is accessed by law enforcement authorities, as underlined in the previous opinion issued by the WP29²⁸.

5 CONCLUSION

105. The EDPB **welcomes the efforts made by the U.S. authorities and the Commission to implement the Privacy Shield, especially actions undertaken to adapt the initial certification process, start ex officio oversight and enforcement actions**, as well as the efforts made by the U.S Government by publishing a number of important documents **and the appointment of a new Chair as well as of two new members of the PCLOB, meaning that the PCLOB has reached the required quorum for its functioning.**
106. However, **the EDPB still has a number of significant concerns that need to be addressed by both the Commission and the U.S. authorities.**
107. **The absence of substantial checks remains a concern of the EDPB. Other areas that require further attention are the application of the Privacy Shield requirements regarding onward transfers, HR Data and processors, as well as the recertification process.** In addition, the EDPB recalls the **remaining issues** with respect to certain elements of the commercial part of the Privacy Shield adequacy decision as already raised in the WP 29’s Opinion 01/2016.
108. As regards the **collection of data by public authorities, the EDPB can only encourage the PCLOB to issue further reports**, including on PPD-28 to follow up on the first report in order to provide additional elements as to how the safeguards of PPD-28 are applied, on Section 702 FISA, and Executive Order 12333.
109. **On the Ombudsperson mechanism, the EDPB is still awaiting the appointment of a permanent independent Ombudsperson.** Given the elements provided, **the EDPB is not in a position to conclude that the Ombudsperson is vested with sufficient powers to access information and to remedy non-compliance, and it can thus not state that the Ombudsperson can be considered an “effective remedy before a tribunal” in the meaning of Art. 47 of the EU Charter of Fundamental Rights.**

²⁷ A first request from an EU individual was received under the Ombudsperson mechanism at the end of 2018.

²⁸ WP 238

110. Finally, the EDPB recalls that the **same concerns will be addressed by the European Court of Justice in cases that are already pending** before the Court.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

ANNEX TO THE EDPB REPORT ON THE SECOND EU-US PRIVACY SHIELD ANNUAL JOINT REVIEW

Factual findings of the second annual joint review of the EU-US Privacy Shield

GENERAL INFORMATION

1. The U.S. Delegation was composed of high level representatives.
2. As of now, the Privacy Shield List contains around 3944 organizations, 338 are on the “Inactive” List either because they have withdrawn from the program (38), not recertified or because their certification has lapsed. There was no case where an organization was removed from the List because it persistently failed to comply.
3. GDPR has led to an increase of interest in the Privacy Shield. The DoC has about 1000 more certifications under review.
4. The DoC has increased their staff to 12 persons now that exclusively work on the Privacy Shield.

1 ON COMMERCIAL ASPECTS

1.1 Self-Certification Process and Cooperation between U.S. authorities in the Privacy Shield Program

5. The DoC reviews all self-certifications (first time applicants as well as recertification submissions) for:
 1. Registration with IRM
 2. Payment of Annex I Arbitral Fund Contribution
 3. Compliance with supplemental principle 6
 4. Completion and consistency of certification information
 5. Privacy notices
6. DoC has not finalized 100 first-time certifications and 30 re-certifications because the requirements set out by the Privacy Shield were not fulfilled.
7. As regards the depth of the analysis the DoC performs: the DoC checks the applications for inconsistencies between the privacy policy and the certification (For example HR/NON HR). It does not check if the data transferred is necessary and proportionate to the purpose because they consider that the Privacy Shield does not go into this level of detail.
8. In order to address the concern expressed by the WP29 regarding the duty of the certifying organization to publish their privacy policy referring to the Privacy Shield certification before the DoC has completed the exercise of checking and listing the organization, the DoC has changed the procedure.
9. The DoC now:
 - Prohibits a first-time applicant from making public representations about participation until the PS Team approves its certification
 - Requires an applicant to submit a draft privacy policy for review

- Directs an applicant to remove any premature references
10. As the practical experience with the certification process increases the DoC has refined their procedures and now for example have produced more guidance for the review of applications regarding the identification of foreign entities; they ask the companies for more precise links so individuals could more easily exercise their rights, they ask for more than one point of contact within the organization to make sure messages from the DoC are received.
 11. 2 weeks before a certification reaches its next certification due date, the DoC sends the organization a notice to remind them of the need to re-certify if the organization wishes to stay on the “active” List.
 12. The organizations that want to stay in the Privacy Shield program are obliged to communicate their re-certification by the due date.
 13. However, the re-certification process is usually not finished by the due date which leads to organizations being listed as “active” while the due date for re-certification has “expired”. A very common reason for this is for example an unpaid fee. The DoC then has to go back to the organization to explain what needs to be done.
 14. The DoC emphasized that even if the due date for re-certification on the Privacy Shield list is in the past, there is no gap in the protection because the protection is provided by the public commitments made by the organizations.
 15. However they agreed that this situation might be confusing for companies or individuals checking the listing of an organization and seemed to agree that it would at a minimum be helpful if the Privacy Shield website itself would provide an explanation on why an organization is still on the “active” list while the due date for the re-certification has expired.
 16. Once the organization has submitted its application for re-certification it is required to complete its certification within 45 days. If it fails to meet this deadline, it is required to remove any references to its participation in the Privacy Shield Program and it might face referral to the FTC.

[1.2 Oversight and supervision of compliance with the principles - Activities by the DoC](#)

17. On a quarterly basis the DoC identifies organizations that have started but not finished an initial or re-certification or that did not submit their annual re-certification at all.
18. The identified organizations receive a certified letter from the DoC, warning them of potential referrals to the FTC or DoT if they do not fulfil outstanding requirements or to withdraw properly from the program. The DoC informs the FTC/DoT of its intent to send those letters. The organizations have 30 days to respond to the letter. The DoC compiles a list of those organizations that fail to take action and respond to the letter. This procedure has led to 100 referrals from the DoC to the FTC, 56 of those referral were made in the second year of the Privacy Shield program. DoC and FTC/DoT cooperate throughout the whole process. Simultaneously with the referral an organization is (at least temporarily) removed from the “active” Privacy Shield List.
19. As foreseen in the Privacy Shield text, the DoC also performs random web searches for false claims of participation in the program. Those web-searches have only led to few cases that were referred to the FTC.

20. The DoC has performed a sweep of 100 randomly chosen organizations. The focus of the sweep was the accessibility of the Privacy Policy, the responsiveness of the organization and the availability of the IRM. The DoC sent more in-depth compliance questionnaires to 21 organizations that showed minor or more significant peculiarities (for example: No response from designated point of contact; Privacy policy was no longer accessible online; Missing references to one or more elements of the notice principle). The organizations must respond within 30 days. If the response is not satisfactory, the organizations – similar to the procedure described above – receive a certified warning letter requiring the organization to indicate within a 30 day period how it has addressed the concerns. If those are not resolved within the 30 days the organization is moved to the “inactive” list and the case is being referred to the FTC or DoT. It was confirmed that even if the case was resolved within the 30 days the DoC could refer it to the FTC.
21. As an example, the DoC indicated that Facebook and Cambridge Analytica were for instance removed from the list for some processing because they lapsed.
22. In addition, the DoC clarified that concerning the Facebook data breach, the certificate to the Privacy Shield of Facebook does not cover the platform from which the app accessed the data.
23. The DoC has also designated 1 person to follow the media and to do keyword searches to identify possible breaches of the Privacy Shield commitments.
24. The DoC also performs regular checks for broken links to the privacy policy on the Privacy Shield list.
25. The DoC has not made use of its right to request a copy of the relevant privacy provisions of an organizations contract with an agent.
26. **European Commission and EDPB representatives' presentations** The European Commission, EDPB Chair and representatives gave a short presentation on the updates about the work done on the European Union side.

1.3 Oversight and supervision of compliance with the principles - Activities by the FTC

27. FTC now has 5 commissioners again.
28. The new commission is organizing hearings on Competition and Consumer Protection in the 21st Century which will also cover the existing and possible extension of the FTC's enforcement powers (<https://www.ftc.gov/policy/advocacy/public-comment-topics-process#5>).
29. In the Division of Privacy and Identity Protection, Bureau of Consumer Protection there are 40 lawyers working only on privacy (a few also work on FOIA) and there are more people from other fields (e.g. tech) that support their work.
30. This year the FTC has brought 5 new Privacy Shield cases: 2 against organizations that did not complete their certification, 3 cases where the certification has lapsed. In most of those cases, the organization failed to verify the deletion, return or continued application of the Privacy Shield Principles to personal data transferred under the Privacy Shield.
31. The FTC has started to send out CIDs (Civil Investigation Demands) proactively to monitor compliance with the Privacy Shield Principles. The FTC could not provide more details on the selected targets or topics of this exercise. In general the FTC has a broad latitude to do sweeps. There is no need for the

FTC to demonstrate that it has a reasonable suspicion. The objective is rather to identify where it is profitable to spend the resources.

32. The FTC still practices the already established procedure to check the cases it investigates for other reasons if the organization is also certified under the Privacy Shield.
33. With regards to the ongoing investigation concerning Facebook and Cambridge Analytica, the FTC was not in a position to share any detail. However, the Chief Council of the DoC shared verbally the content of an early response letter from Facebook in which the company basically presented different points of its line of defence.

[1.4 Oversight and supervision of compliance with the principles - Activities by the DoT](#)

34. Currently there is no airline participating in the Privacy Shield and only very few ticket agents.
35. Because the DoT's situation is very similar to the one of the FTC it looks closely at FTC practice and case law. The DoT has not received any Privacy Shield related complaints so far.

[1.5 Guidance for the companies adhering to the Privacy Shield](#)

36. The DoC has (following informal consultation of members of the ITS at working level) produced guidance on the [Accountability for Onward Transfer Principle](#) and the notion of [Processor](#) and published it on its website

[1.6 IRM](#)

37. The DoC has issued guidance to the IRM in order to have comparable annual reports.
38. The DoC plans to issue guidance on possible conflicts of interest for the next year.
39. Most complaints to the IRM VeraSafe were found ineligible because the complainant was an U.S. resident and the company concerned was also situated in the U.S.
40. As contractually agreed, if there was a breach in the Privacy policy (meaning if the company did not respect its privacy policy, not that the policy itself is in breach of the Privacy Shield), the VeraSafe clients (organizations that certified under the privacy shield) committed to accept VeraSafe's decision to impose a "fine" on them. The "fine" would be paid to the individual that successfully claimed a breach.

[1.7 Arbitral Panel](#)

41. The fee, that according to the Privacy Shield text is collected from the certified organizations annually is actually only collected once at the initial certification. The collected amount (under Safe Harbor and the Privacy Shield) totals to 4.5 million \$.
42. Arbitral panel procedure has never been triggered so far. The question is if the fee should still be collected. Recommendation of the Arbitral Administrator Association (that manages the fund) is to not change anything for now since there is no figure on how much the handling of an average case would cost.

[1.8 Automated Decision Making](#)

43. The COM presented the main elements of a study commissioned to an independent contractor.

44. The study came to the conclusion that automated decisions making (in the narrow GDPR definition of decisions having legal effects on individuals), these decisions are not taken on the basis of data transferred from the EU. Such decisions are more likely to take place in “EU customer facing” situations (i.e. where the US company directly targets EU customers).
45. However, the study at the same time underlines that this is a fast developing area which has to be closely monitored in the future.
46. In the rare situation where ADM are made (for example in the context of credit lending, housing, employment), cases where personal data transferred from the EU are used is quite limited.
47. Some private companies who participated in the joint review exercise (such as Workday and Salesforce) confirmed that they are offering services to their customers (EU businesses) which can be AI-based and potentially conduct some automated decisions²⁹. However, these companies insisted that in any case they always act as data processors under the instructions of data controllers based in the EU.
48. According to the study, several credit-reporting agencies have self-certified under Privacy Shield (notably Experian, one of the three big major reporting companies in the US). The FTC has general enforcement jurisdiction over these agencies, in cooperation with the US Consumer financial bureau, which has supervisory authority over credit-reporting agencies (such companies have different products - some of these products may fall under the US Fair Credit Reporting Act). The Consumer financial bureau would pass on cases to the FTC so the same principles apply to such companies and if they are misrepresented the FTC would enforce them.
49. FTC publicly announced that they are investigating Equifax.
50. The US FTC presented the case about “Realpage”, a background screening company doing criminal checks which was conducting automated decisions making by using weak accuracy verification methods (if the last name and the first three letters of the firstname of an individual matched a criminal record, Realpage would consider this enough to identify the individual as criminal). The FTC asked the company to put in place a better, reasonable procedure to ensure firstnames’ accuracy. The case led to a 3 million dollars fine settlement³⁰.
51. There was no other significant new developments as regards Automated Decision Making to take note of.

1.9 HR Data

52. Since the work on guidance regarding the processing of employment data within the last year was not successful this year’s review focused less on the definition of HR data but rather on the consequences the different definitions lead to: The worry on the EU side being, that additional protections granted by the Privacy Shield for employment data (Opt In in marketing purposes rather than opt out) would

²⁹ See for example the “Prism Analytics” tool offered by Workday which allows companies to “bring data in at scale from any source and prepare, analyze and securely share it with[in the] organization” (see <https://www.workday.com/en-us/applications/prism-analytics.html>) and the AI-based predictive marketing tool “Einstein” proposed by Salesforce (see: <https://www.salesforce.com/products/einstein/overview/>).

³⁰ See: <https://www.ftc.gov/enforcement/cases-proceedings/152-3059/realpage-inc>

not fall under anyone's jurisdiction. Given the wording of the Privacy Shield, the discussions on different possible readings of this need to continue.

2 ON GOVERNMENT ACCESS TO PERSONAL DATA: RELEVANT DEVELOPMENTS IN THE U.S. LEGAL FRAMEWORK AND TRENDS

53. Legal framework has not changed substantially.

2.1 Reauthorisation of 702 FISA

54. The U.S. government reported about the amendments authorized by the FISA Amendments Reauthorization Act of 2017.
55. In particular, further explanation was provided about the possibility to reintroduce "about collection". It was stressed that, if the governments were to re-introduce "about collection" under the UPSTREAM programme, it would be required to take particularly demanding procedural steps (implying authorizations by the Court and the Congress), and where the FISA Court would be expected to appoint an amicus curiae when such an application is made.
56. The U.S. government also reported about the several transparency requirements, including semi-annual reports, which – together with additional material – is made available on a new website: <https://www.intel.gov/intel-vault>.

2.2 PPD-28

57. The U.S. government published a response to the recently published (in redacted form) report by the PCLOB. It disagrees with the PCLOB on the question of whether the scope of application of PPD28 is sufficiently clear for the agencies to apply it (PCLOB expressing doubts in the said report).
58. The U.S. government confirmed that the safeguards of PPD-28 also apply for personal data collected under 702 FISA. This would include safeguards related to the retention of data, their dissemination, and specifications on the targeting with regard to the purpose of collecting foreign intelligence.

2.3 The Ombudsperson mechanism and the EU individual complaint handling body

59. Acting Under Secretary of State for Economic Growth, Energy, and the Environment and Acting Privacy Shield Ombudsperson, Manisha Singh, explained the procedures set up to make the Ombudsperson mechanism under the Privacy Shield work, including how a case would be handled in theory. No further declassified information was shared as to the rules of procedure of how she cooperates with the intelligence community. She assured she would not sign a response letter to the requestor if she were not convinced of the findings presented to her. It was confirmed during the discussion that, in response to an Ombudsperson request, she would be provided with a report from the Intelligence Community (IC) in order to provide oversight and to take actions (without being able to directly access information or directly remedy non-compliance). She also stressed that she would have the ability to escalate the matter to the Secretary of State in order to assure that her demands are met.
60. The European Centralised Body (EUCB) presented its rules of procedure, explaining how a request would be handled before submitted to the Ombudsperson.

61. A representative of the Intelligence Community (IC) confirmed that the Inspector General of the ODNI would always be informed when a request would be forwarded to the ODNI by the Ombudsperson.
62. As the remedying of a possible violation, the U.S. government clarified that any violation of FISA would also have to be reported to the FISA court.

2.4 PCLOB

63. Shortly before the second annual review, the Senate confirmed three members of the PCLOB. As President Trump appointed those candidates on 16 October 2018, the PCLOB has reached quorum again. Two additional candidates have been nominated and are awaiting their confirmation by the U.S. Senate.
64. In addition, also shortly before the joint review, the PCLOB published a redacted version of its report on PPD-28. The government also published a response to that report.
65. The new PCLOB will have to decide about the declassification of report on Executive Order 12333 finalized under the previous PCLOB Chair.
66. As regards other reports to be done, and possible reviews of previous report, such as on section 702, the new PCLOB would have to determine in the coming times its work plan and schedule.

2.5 Inspector General (IG) of the ODNI

67. The new IG was sworn in on 17 May 2018. He stressed his independence and the fact that he has full access to (classified) documents in the IC community, which would as a matter of fact never be restrained.
68. He clarified that usually indirect access to information would be sought through reports from the IC community, but that the IG has direct access as well, if needed.
69. He also confirmed that IG, in principle, has discretion whether to act and would follow set priorities, but that requests by the Ombudsperson would in the current setting always be considered as of particular importance.

2.6 Redress

70. The U.S. government presented recent case law of the FISA court and referred to the website of the FISA court, where redacted decisions are published.
71. Related to the procedural requirement of “standing”, the U.S. government reported about the ACLU case, decided by different FISA “chambers” and finally on the appellate level. It deals with an unusual case, where ACLU was seeking the publication of FISA court decisions, based on a right of public access to documents. The court had denied in the first instance that ACLU would have standing. Finally, the FISA Court of Review court said it would.
72. No further developments could be presented on the requirement of standing in other relevant cases, as the Wikimedia case is still pending. With regard to legal claims relying on a violation of FISA, the U.S. Government referred to the possibility of making a Freedom of Information (FOIA) request first.
73. The U.S. confirmed that PPD-28 does not create rights enforceable before a court. Consequently, cases would have to be brought to the attention of the IG or the Ombudsperson.

2.7 Additional information on access to data by law enforcement authorities

74. The U.S. government reported about a Department of Justice memo on the Stored Communications Act³¹. The purpose of the memo would be to further harmonize the use of such applications to the court which prohibit providers to disclose the order. According to the new memo, such applications have to be further justified by the prosecutors seeking such order, and a general limit of 1 year for such orders is foreseen, with exceptions that need to be justified again.
75. The U.S. government also reported about the Supreme Court ruling in the Carpenter case, in which a suspect was prosecuted on the basis cellphone location records, without a search warrant. The Supreme Court ruled that the evidence was illegally acquired and not receivable in court, since the suspect had a reasonable expectation of privacy for these data so that the government had violated the Fourth Amendment to the United States Constitution by accessing the cellphone location records without a search warrant.³²

³¹ Stored Communications Act (SCA, codified at 18 U.S.C. Chapter 121 §§ 2701–2712) is a law that addresses voluntary and compelled disclosure of "stored wire and electronic communications and transactional records" held by third-party internet service providers (ISPs).

³² Carpenter v. United States, 138 S. Ct. 2206

Opinion of the Board (Art. 64)



EDPB Plenary Meeting, 22-23 January 2019

Opinion 01/2019 on the draft list of the competent supervisory authority of the Principality of Liechtenstein regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)

Adopted on 23 January 2019

Table of contents

1	Summary of the Facts.....	4
2	Assessment.....	5
2.1	General reasoning of the EDPB regarding the submitted list	5
2.2	Application of the consistency mechanism to the draft list	6
2.3	Analysis of the draft list	6
	BIOMETRIC DATA	6
	GENETIC DATA.....	6
	PROCESSING USING INNOVATIVE TECHNOLOGY	6
	SYSTEMATIC TRACKING	7
	COMBINING OR MATCHING PERSONAL DATA OBTAINED FROM MULTIPLE SOURCES AND FURTHER PROCESSING THEREOF.....	7
	SYSTEMATIC WORKPLACE MONITORING	7
	EXCEPTIONS TO INFORMATION TO BE PROVIDED TO THE DATA SUBJECT ACCORDING TO ARTICLE 14.5 GDPR	7
	DENIAL OF SERVICE BASED (NOT SOLELY) ON AUTOMATED DECISION-MAKING (INCLUDING PROFILING)	8
	PROCESSING OF PERSONAL DATA IF THE DATA ARE EVALUATED, PROCESSED AND USED BY THE AUTHORITIES CONCERNED AND FORWARDED TO LAW ENFORCEMENT AUTHORITIES.....	8
3	Conclusions / Recommendations.....	8
4	Final Remarks	9

The European Data Protection Board

Having regard to Article 63, Article 64 (1a), (3) - (8) and Article 35 (1), (3), (4), (6) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereafter "GDPR"),

Having regard to Article 51 (1b) of Directive 2016/680 EU on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (hereafter "Law Enforcement Directive").

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018, as revised on 23 November 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (hereafter GDPR) throughout the European Economic Area. In compliance with article 64.1 GDPR, the Board shall issue an opinion where a supervisory authority (SA) intends to adopt a list of processing operations subject to the requirement for a data protection impact assessment pursuant to article 35.4 GDPR. The aim of this opinion is therefore to create a harmonised approach with regard to processing that is cross border or that can affect the free flow of personal data or natural person across the European Union. Even though the GDPR doesn't impose a single list, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by requesting SAs to include some types of processing in their lists, secondly by requesting them to remove some criteria which the Board doesn't consider as necessarily creating high risks for data subjects, and finally by requesting them to use some criteria in a harmonized manner.

(2) With reference to Article 35 (4) and (6) GDPR, the competent supervisory authorities shall establish lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment (hereinafter "DPIA"). They shall, however, apply the consistency mechanism where such lists involve processing operations, which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

(3) While the draft lists of the competent supervisory authorities are subject to the consistency mechanism, this does not mean that the lists should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB assessment/opinion is not to reach a single EU list but rather to avoid significant inconsistencies that may affect the equivalent protection of the data subjects.

(4) The carrying out of a DPIA is only mandatory for the controller pursuant to Article 35 (1) GDPR where processing is “likely to result in a high risk to the rights and freedoms of natural persons”. Article 35 (3) GDPR illustrates what is likely to result in a high risk. This is a non-exhaustive list. The Working Party 29 in the Guidelines on data protection impact assessment¹, as endorsed by the EDPB², has clarified criteria that can help to identify when processing operations are subject to the requirement for a DPIA. The Working Party 29 Guidelines WP248 state that in most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out, however, in some cases a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

(5) The lists produced by the competent supervisory authorities support the same objective to identify processing operations likely to result in a high risk and processing operations, which therefore require a DPIA. As such, the criteria developed in the Working Party 29 Guidelines should be applied when assessing whether the draft lists of the competent supervisory authorities does not affect the consistent application of the GDPR.

(6) Twenty-two competent supervisory authorities received an opinion on their draft lists from the EDPB on 5 September 2018. A further 4 SAs received an opinion on their draft lists on 7 December 2018.

(7) The opinion of the EDPB shall be adopted pursuant to Article 64 (3) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. The competent supervisory authority of the Principality of Liechtenstein has submitted its draft list to the EDPB. The decision on the completeness of the file was taken on 29 October 2018.
2. The period until which the opinion has to be adopted has been extended until 5 February 2019 taking into account the complexity of the subject matter, in particular the need to factor in the outcome of the review of the twenty-six draft lists previously submitted by competent supervisory authorities and the need for a global assessment of all of them.

¹ WP29, Guidelines on Data Protection Impact Assessment and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 (WP 248 rev. 01).

² EDPB, Endorsement 1/2018.

2 ASSESSMENT

2.1 General reasoning of the EDPB regarding the submitted list

3. Any list submitted to the EDPB has been interpreted as further specifying Art 35.1, which will prevail in any case. Thus, no list can be exhaustive.
4. In compliance with article 35.10 GDPR, the Board is of the opinion that if a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of the legal basis the obligation to carry out a DPIA in accordance with paragraphs 1 to 7 of article 35 GDPR does not apply, unless the Member State deems it necessary.
5. Further, if the Board requests a DPIA for a certain category of processing and an equivalent measure is already required by national law, the Data Protection Office of the Principality of Liechtenstein (hereafter Liechtenstein Supervisory Authority) shall add a reference to this measure.
6. This opinion does not reflect upon items submitted by the Liechtenstein Supervisory Authority, which were deemed outside the scope of Article 35.6 GDPR. This refers to items that neither relate “to the offering of goods or services to data subjects” in several Member States nor to the monitoring of the behaviour of data subjects in several Member States. Additionally, they are not likely to “substantially affect the free movement of personal data within the Union”. This is especially the case for items relating to national legislation and in particular where the obligation to carry out a DPIA is stipulated in national legislation. Further, any processing operations that relate to law enforcement were deemed out of scope, as they are not in scope of the GDPR.
7. The Board has noted that several supervisory authorities have included in their lists some types of processing which are necessarily local processing. Given that only cross border processing and processing that may affect the free flow of personal data and data subjects are concerned by Article 35.6 GDPR, the Board will not comment on those local processing.
8. The Board notes that types of processing which fall within the scope of the Law Enforcement Directive are by definition not subject to article 35.6 GDPR, however the Board may issue recommendations based on article 51 (1b) of the Law Enforcement Directive.
9. The opinion aims at defining a consistent core of processing operations that are recurrent in the lists provided by the SAs.
10. This means that, for a limited number of types of processing operations that will be defined in a harmonised way, all the Supervisory Authorities will require a DPIA to be carried out and the Board will recommend the SAs to amend their lists accordingly in order to ensure consistency.
11. When this opinion remains silent on DPIA list entries submitted, it means that the Board is not asking the Liechtenstein Supervisory Authority to take further action.
12. Finally, the Board recalls that transparency is key for data controllers and data processors. In order to clarify the entries in the list, the Board is of the opinion that making an explicit reference in the lists, for each type of processing, to the criteria set out in the guidelines could improve this transparency. Therefore, the Board considers that an explanation on which criteria have been taken into account by the Liechtenstein Supervisory Authority to create its list could be added.

2.2 Application of the consistency mechanism to the draft list

13. The draft list submitted by the Liechtenstein Supervisory Authority relates to the offering of goods or services to data subjects, relates to the monitoring of their behaviour in several Member States and/or may substantially affect the free movement of personal data within the Union mainly because the processing operations in the submitted draft list are not limited to data subjects in this country.

2.3 Analysis of the draft list

14. Taking into account that:
 - a. Article 35 (1) GDPR requires a DPIA when the processing activity is likely to result in a high risk to the rights and freedoms of natural persons; and
 - b. Article 35 (3) GDPR provides a non-exhaustive list of types of processing that require a DPIA, the Board is of the opinion that:

BIOMETRIC DATA

15. The list submitted by the Liechtenstein Supervisory Authority for an opinion of the Board states, that the extensive processing of biometric data falls under the obligation to perform a DPIA on its own. The Board is of the opinion that the processing of biometric data is not necessarily likely to represent a high risk per se. However, the processing of biometric data for the purpose of uniquely identifying a natural person in conjunction with at least one other criterion requires a DPIA to be carried out. The Board is of the opinion that the wording used to describe the type of processing is not clear enough. Either the extensive nature of the processing means that the processing is made on a large scale, in which case the description should be modified to clearly make a reference to this criterion, or it just means that the criterion is systematically used, in which case another criterion should be added to ensure consistency.

GENETIC DATA

16. The list submitted by the Liechtenstein Supervisory Authority for an opinion of the Board does not currently require a DPIA to be done for the processing of genetic data. The Board is of the opinion that the processing of genetic data is not necessarily likely to represent a high risk per se. However, the processing of genetic data in conjunction with at least one other criterion requires a DPIA to be carried out. Therefore, the Board requests the Liechtenstein Supervisory Authority to amend its list accordingly, by adding explicitly the processing of genetic data in conjunction with at least one other criterion to its list, to be applied without prejudice to article 35(3) GDPR.

PROCESSING USING INNOVATIVE TECHNOLOGY

17. The list submitted by the Liechtenstein Supervisory Authority for an opinion of the Board envisages that the use of innovative technology, on its own, requires a DPIA. The Board is of the opinion that the use of innovative technology is not necessarily likely to represent a high risk per se. However, the use of innovative technology in conjunction with at least one other criterion requires a DPIA to be carried out. Therefore, the Board requests the Liechtenstein Supervisory Authority to amend its list accordingly, by adding that the item requires a DPIA to be carried out only when it is done in conjunction with at least one other criterion.

SYSTEMATIC TRACKING

18. The Board recalls that systematic tracking is a factor in determining the likelihood of high risk, however does not necessarily lead to a likely high risk per se. However, where systematic tracking occurs in conjunction with at least one other criterion, a DPIA should be carried out. The list submitted by the Liechtenstein Supervisory Authority for an opinion of the Board does currently require a DPIA to be carried out when systematic tracking of data subjects occurs. The Board requests the Liechtenstein Supervisory Authority to amend its list accordingly, by requiring a DPIA to be carried out in cases of systematic tracking of data subjects only when it is done in conjunction with at least one other criterion.

COMBINING OR MATCHING PERSONAL DATA OBTAINED FROM MULTIPLE SOURCES AND FURTHER PROCESSING THEREOF

19. The Board recalls that matching or combining datasets is a factor in determining the likelihood of high risk, however in its view combining or matching of personal data obtained from multiple sources does not lead to a likely high risk per se. The Board further recalls that in its view further processing of personal data should not be a criterion leading to an obligation to do a DPIA, alone or with another criterion. The list submitted by the Liechtenstein Supervisory Authority for an opinion of the Board does currently require a DPIA to be carried out when combining or matching of personal data obtained from multiple sources and further processing thereof occurs. The Board requests the Liechtenstein Supervisory Authority to amend its list accordingly, by requiring a DPIA to be carried out in case of combining or matching of personal data obtained from multiple sources only when occurring in conjunction with at least one other criterion.

SYSTEMATIC WORKPLACE MONITORING

20. The Board takes note of the inclusion of “systematic workplace monitoring” in the Liechtenstein DPIA list. The Board recalls that in its view WP249 of the Article 29 working party remain valid when defining the concept of systematic processing of employee data.

EXCEPTIONS TO INFORMATION TO BE PROVIDED TO THE DATA SUBJECT ACCORDING TO ARTICLE 14.5 GDPR

21. The Board is of the opinion that types of processing activities that could deprive the data subjects from their rights do not represent a high risk per se. Therefore, a processing activity conducted by the controller under article 14 GDPR and where the information to be given to the data subjects is subject to an exemption under article 14.5 (b) could require a DPIA to be carried out only in conjunction with at least one other criterion. The list submitted by the Liechtenstein Supervisory Authority for an opinion of the Board does currently require a DPIA to be done for the processing of data where article 14(5), para (b) applies extensively. The Board is of the opinion that the wording used to describe the type of processing is not clear enough. Either the extensive nature of the processing means that the processing is made on a large scale, in which case the description should be modified to clearly make a reference to this criterion, or it just means that the criterion is systematically used, in which case another criterion should be added to ensure consistency.

DENIAL OF SERVICE BASED (NOT SOLELY) ON AUTOMATED DECISION-MAKING (INCLUDING PROFILING)

22. The list submitted by the Liechtenstein Supervisory Authority for an opinion of the Board states, that the processing activities which lead to a denial of service, when based, but not solely, on an automated decision (including profiling) fall under the obligation to perform a DPIA. The Board is of the opinion that the reference to automated decision-making does not count as a second criterion in this case, since the description states that the processing which include a human intervention are also included. This means that any processing that end up with a denial of service are subject to the obligation to do a DPIA. The Board therefore requests the Liechtenstein Supervisory Authority to amend its list accordingly, by adding that the item referencing the processing which may lead to denial of service based (not solely) on automated decision-making (including profiling) requires a DPIA to be carried out only when it is done in conjunction with at least one other criterion.

PROCESSING OF PERSONAL DATA IF THE DATA ARE EVALUATED, PROCESSED AND USED BY THE AUTHORITIES CONCERNED AND FORWARDED TO LAW ENFORCEMENT AUTHORITIES

23. The list submitted by the Liechtenstein Supervisory Authority for an opinion of the Board states, that the processing activities which are further transmitted to law enforcement fall under the obligation to perform a DPIA. The Board takes note that those processing operations will not always fall within the scope of the Law Enforcement Directive: whistle blowing processing for example, will fall under this criterion and will therefore require a DPIA. The Board acknowledges that the fact that data will likely be forwarded to law enforcement authorities can be a factor in determining the likelihood of high risk, however it does not necessarily lead to a likely high risk per se. The Board therefore requests the Liechtenstein Supervisory Authority to amend its list accordingly, by adding that the item referencing the processing when data are evaluated, processed and used by the authorities concerned and forwarded to law enforcement authorities requires a DPIA to be carried out only when it is done in conjunction with at least one other criterion.

3 CONCLUSIONS / RECOMMENDATIONS

24. The draft list of the Liechtenstein Supervisory Authority may lead to an inconsistent application of the requirement for a DPIA and the following changes need to be made:

- Regarding biometric data: the Board requests the Liechtenstein Supervisory Authority to amend its list by adding explicitly the processing of biometric data for the purpose of uniquely identifying a natural person in conjunction with at least one other criterion to its list;
- Regarding genetic data: the Board requests the Liechtenstein Supervisory Authority to amend its list by adding explicitly the processing of genetic data in conjunction with at least one other criterion to its list;
- Regarding processing using new or innovative technology: the Board requests the Liechtenstein Supervisory Authority to amend its list by adding that the item requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion;
- Regarding systematic tracking: the Board requests the Liechtenstein Supervisory Authority to amend its list by adding that the item requires a DPIA to be carried out only when it is done in conjunction with at least one other criterion;

- Regarding combining or matching of personal data obtained from multiple sources and further processing thereof: the Board requests the Liechtenstein Supervisory Authority to amend its list by firstly removing the reference to further processing and secondly by adding that the item requires a DPIA to be carried out only when it is done in conjunction with at least one other criterion;
- Regarding exceptions to information to be provided to the data subject according to Art. 14.5 GDPR: the Board request the Liechtenstein Supervisory Authority to amend its list either by clarifying that the extensive nature of the processing means that the processing is made on a large scale or, if it just means that the criterion is systematically used, by adding that the item requires a DPIA to be carried out only when it is done in conjunction with at least one other criterion;
- Regarding denial of service based (not solely) on automated decision making (including profiling): the Board requests the Liechtenstein Supervisory Authority to amend its list by adding that the item requires a DPIA to be carried out only when it is done in conjunction with at least one other criterion;
- Regarding the data evaluated, processed and used by the authorities concerned and forwarded to law enforcement authorities: the Board requests the Liechtenstein Supervisory Authority to amend its list by adding that the item requires a DPIA to be carried out only when it is done in conjunction with at least one other criterion

4 FINAL REMARKS

25. This opinion is addressed to the Data Protection Office of the Principality of Liechtenstein (Liechtenstein Supervisory Authority) and will be made public pursuant to Article 64 (5b) GDPR.
26. According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Adopted

Opinion of the Board (Art. 64)



EDPB Plenary Meeting, 22-23 January 2019

Opinion 2/2019 on the draft list of the competent supervisory authority of Norway regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)

Adopted on 23 January 2019

Table of contents

1	Summary of the Facts.....	4
2	Assessment.....	5
2.1	General reasoning of the EDPB regarding the submitted list	5
2.2	Application of the consistency mechanism to the draft list	5
2.3	Analysis of the draft list	6
	SCOPE OF THE DRAFT DECISION	6
	EMPLOYEE MONITORING	6
3	Conclusions / Recommendations.....	6
4	Final Remarks	6

Adopted

2

The European Data Protection Board

Having regard to Article 63, Article 64 (1a), (3) - (8) and Article 35 (1), (3), (4), (6) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereafter "GDPR"),

Having regard to Article 51 (1b) of Directive 2016/680 EU on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (hereafter "Law Enforcement Directive").

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018, revised on 23 November 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (hereafter GDPR) throughout the European Economic Area. In compliance with article 64.1 GDPR, the Board shall issue an opinion where a supervisory authority (SA) intends to adopt a list of processing operations subject to the requirement for a data protection impact assessment pursuant to article 35.4 GDPR. The aim of this opinion is therefore to create a harmonised approach with regard to processing that is cross border or that can affect the free flow of personal data or natural person across the European Union. Even though the GDPR doesn't impose a single list, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by requesting SAs to include some types of processing in their lists, secondly by requesting them to remove some criteria which the Board doesn't consider as necessarily creating high risks for data subjects, and finally by requesting them to use some criteria in a harmonized manner.

(2) With reference to Article 35 (4) and (6) GDPR, the competent supervisory authorities shall establish lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment (hereinafter "DPIA"). They shall, however, apply the consistency mechanism where such lists involve processing operations, which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

(3) While the draft lists of the competent supervisory authorities are subject to the consistency mechanism, this does not mean that the lists should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB assessment/opinion is not to reach a single EU list but rather to avoid significant inconsistencies that may affect the equivalent protection of the data subjects.

(4) The carrying out of a DPIA is only mandatory for the controller pursuant to Article 35 (1) GDPR where processing is “likely to result in a high risk to the rights and freedoms of natural persons”. Article 35 (3) GDPR illustrates what is likely to result in a high risk. This is a non-exhaustive list. The Working Party 29 in the Guidelines on data protection impact assessment¹, as endorsed by the EDPB², has clarified criteria that can help to identify when processing operations are subject to the requirement for a DPIA. The Working Party 29 Guidelines WP248 state that in most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out, however, in some cases a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

(5) The lists produced by the competent supervisory authorities support the same objective to identify processing operations likely to result in a high risk and processing operations, which therefore require a DPIA. As such, the criteria developed in the Working Party 29 Guidelines should be applied when assessing whether the draft lists of the competent supervisory authorities does not affect the consistent application of the GDPR.

(6) Twenty-two competent supervisory authorities received an opinion on their draft lists from the EDPB on 5 September 2018. A further 4 SAs received an opinion on their draft lists on 7 December 2018.

(7) The opinion of the EDPB shall be adopted pursuant to Article 64 (3) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. The competent supervisory authority of Norway has submitted its draft list to the EDPB. The decision on the completeness of the file was taken on 22 November 2018.
2. The period until which the opinion has to be adopted has been extended until 1 March 2019 taking into account the complexity of the subject matter, in particular the need to factor in the outcome of the review of the twenty-six draft lists previously submitted by competent supervisory authorities and the need for a global assessment of all of them.

¹ WP29, Guidelines on Data Protection Impact Assessment and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 (WP 248 rev. 01).

² EDPB, Endorsement 1/2018.

2 ASSESSMENT

2.1 General reasoning of the EDPB regarding the submitted list

3. Any list submitted to the EDPB has been interpreted as further specifying Art 35.1, which will prevail in any case. Thus, no list can be exhaustive.
4. In compliance with article 35.10 GDPR, the Board is of the opinion that if a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of the legal basis the obligation to carry out a DPIA in accordance with paragraphs 1 to 7 of article 35 GDPR does not apply, unless the Member State deems it necessary.
5. Further, if the Board requests a DPIA for a certain category of processing and an equivalent measure is already required by national law, the Datatilsynet (hereafter Norwegian Supervisory Authority) shall add a reference to this measure.
6. This opinion does not reflect upon items submitted by the Norwegian Supervisory Authority, which were deemed outside the scope of Article 35.6 GDPR. This refers to items that neither relate “to the offering of goods or services to data subjects” in several Member States nor to the monitoring of the behaviour of data subjects in several Member States. Additionally, they are not likely to “substantially affect the free movement of personal data within the Union”. This is especially the case for items relating to national legislation and in particular where the obligation to carry out a DPIA is stipulated in national legislation. Further, any processing operations that relate to law enforcement were deemed out of scope, as they are not in scope of the GDPR.
7. The Board has noted that several supervisory authorities have included in their lists some types of processing which are necessarily local processing. Given that only cross border processing and processing that may affect the free flow of personal data and data subjects are concerned by Article 35.6, the Board will not comment on those local processing.
8. The opinion aims at defining a consistent core of processing operations that are recurrent in the lists provided by the SAs.
9. This means that, for a limited number of types of processing operations that will be defined in a harmonised way, all the Supervisory Authorities will require a DPIA to be carried out and the Board will recommend the SAs to amend their lists accordingly in order to ensure consistency.
10. When this opinion remains silent on DPIA list entries submitted, it means that the Board is not asking the Norwegian Supervisory Authority to take further action.
11. Finally, the Board recalls that transparency is key for data controllers and data processors. In order to clarify the entries in the list, the Board is of the opinion that making an explicit reference in the lists, for each type of processing, to the criteria set out in the guidelines could improve this transparency.

2.2 Application of the consistency mechanism to the draft list

12. The draft list submitted by the Norwegian Supervisory Authority relates to the offering of goods or services to data subjects, relates to the monitoring of their behaviour in several Member States and/or may substantially affect the free movement of personal data within the Union mainly because the processing operations in the submitted draft list are not limited to data subjects in this country.

2.3 Analysis of the draft list

13. Taking into account that:
 - a. Article 35 (1) GDPR requires a DPIA when the processing activity is likely to result in a high risk to the rights and freedoms of natural persons; and
 - b. Article 35 (3) GDPR provides a non-exhaustive list of types of processing that require a DPIA, the Board is of the opinion that:

SCOPE OF THE DRAFT DECISION

14. The Norwegian DPIA list states that its list includes processing activities that the Norwegian DPA considers to be of high risk to the rights and freedoms of data subjects. However, the Board recalls that the GDPR states that the list that have to be published by the supervisory authorities are the lists of processing that are likely to result in a high risk for the rights and freedoms of data subjects. The Board therefore requests the Norwegian Authority to amend its list by aligning its wording with the wording of Article 35.A of the GDPR.

EMPLOYEE MONITORING

15. The Board takes note of the inclusion of “processing of personal data involving measures for systematic monitoring of employee activities” in the Norwegian DPIA list. The Board recalls that in its view WP249 of the Article 29 working party remain valid when defining the concept of systematic processing of employee data.

3 CONCLUSIONS / RECOMMENDATIONS

16. The draft list of the Norwegian Supervisory Authority may lead to an inconsistent application of the requirement for a DPIA and the following changes need to be made:
 - Regarding the scope of the list: the Board requests the Norwegian Supervisory Authority to amend its list by stating that the types of processing listed are the one that are likely to present high risks for the rights and freedom of data subjects.

4 FINAL REMARKS

17. This opinion is addressed to the Datatilsynet (Norwegian Supervisory Authority) and will be made public pursuant to Article 64 (5b) GDPR.
18. According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Adopted

Statement



Annex I to Statement 2/2019 on the use of personal data in the course of political campaigns

Adopted on 13 March 2019

REFERENCES TO GUIDANCE ISSUED BY DATA PROTECTION AUTHORITIES

Belgium

- Guidance from the BE DPA concerning political campaigns/elections:
 - NL version: <https://www.gegevensbeschermingsautoriteit.be/verkiezingen>
https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/Nota_verkiezingen_AVG.pdf
 - FR version: <https://www.autoriteprotectiondonnees.be/elections>
https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents>Note_elections_RGPD.pdf

EDPS

- EDPS Opinion on online manipulation and personal data:
https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf

France

- Communication politique: quelles sont les règles pour l'utilisation des données issues des réseaux sociaux :
<https://www.cnil.fr/fr/communication-politique-quelles-sont-les-regles-pour-lutilisation-des-donnees-issues-des-reseaux>

Greece

- Political Communication Guidance:
http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/THEMATIKES_ENOTITES/POLITIKA_L_COMMUNICATION_DIRECTIONS_V3.0%20FINAL.PDF

Ireland

- Elections and Canvassing: Data Protection and Electronic Marketing:
<https://www.dataprotection.ie/sites/default/files/uploads/2018-11/Canvassing%20Elected%20Reps%20FINAL.pdf>
- Elections & Canvassing: Data Protection and Electronic Marketing – the data protection rights of individuals: <https://www.dataprotection.ie/sites/default/files/uploads/2018-11/Canvassing%20-%20Individuals%20update%20final%20version.pdf>

Lithuania

- Recommendation on the processing of personal data during elections, prepared by the State Data Protection Inspectorate of the Republic of Lithuania:
[Rekomendacija dėl asmens duomenų tvarkymo rinkimų metu \(2019 m.\)](#)
- Press release on the Recomendation: <https://www.ada.lt/go.php/lit/Valstybine-duomenų-apsaugos-inspekcija-parengė-rekomendacija-apie-asmens-duomenų-tvarkymą-rinkimu-metu/50>

Poland

- Guidelines for political parties and other actors in the electoral process:
<https://uodo.gov.pl/pl/138/497>

Portugal

- Diretriz/2019/1 relativa ao tratamento de dados pessoais no contexto de campanhas eleitorais e marketing político:
https://www.cnpd.pt/bin/decisoes/Diretrizes/Diretriz_1_2019_PropagandaPolitica.pdf

Slovenia

- Guidebook for the organisers of election campaigns:
http://www.mju.gov.si/fileadmin/mju.gov.si/pageuploads/JAVNA_UPRAVA/Volilna_in_referendumска_zakonodaja/Vodnik_za_organizatorje_volilnih_kampanj_2019.pdf

Spain

- Circular 1/2019, de 7 de marzo, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales relativos a opiniones políticas y envío de propaganda electoral por medios electrónicos o sistemas de mensajería por parte de partidos políticos,

federaciones, coaliciones y agrupaciones de electores al amparo del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General:

<https://www.boe.es/boe/dias/2019/03/11/pdfs/BOE-A-2019-3423.pdf>

United Kingdom

- Guidance on political campaigning:
https://ico.org.uk/media/1589/promotion_of_a_political_party.pdf

Statement



Statement 3/2019 on an ePrivacy regulation **Adopted on 13 March 2019**

The European Data Protection Board has adopted the following statement:

The EDPB calls on the EU legislators to intensify efforts towards the adoption of an ePrivacy Regulation, which is necessary to complete the EU's framework for data protection and confidentiality of communications. The EDPB wishes to reiterate the positions previously adopted by data protection authorities in the EU, including the Opinion 1/2017 of the Article 29 Working Party and the Statement adopted on 25 May 2018. The ePrivacy Regulation must under no circumstances lower the level of protection offered by the current ePrivacy Directive 2002/58/EC and must complement the GDPR by providing additional strong guarantees for all types of electronic communications. Far from being an obstacle to the development of new technologies and services, the ePrivacy Regulation is necessary to ensure a level playing field and legal certainty for market operators. The EDPB invites Member States, under the leadership of the Presidency of the Council, to ensure a high level of protection and to proceed to the finalisation of their negotiating position without further delay, so that negotiations with the European Parliament can begin as soon as possible.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Sophie In 't Veld
Member of the European Parliament

Brussels, 15 May 2019

By email only

Ref: C-1123-2019

Subject: Your letter to the EDPB of 17 April 2019

Dear Ms In 't Veld,

Thank you very much for your letter dated 17 April 2019 on the important topic of connected vehicles. Automated and connected vehicles may offer significant benefits for users by providing enhanced levels of usability or convenience, as well as for the general public by improving traffic efficiency and safety of vehicle drivers and their passengers, other road users and pedestrians. In many cases, this will include the processing of personal data due to the wide variety of sensors installed in them, thus raising new challenges to the rights to the protection of personal data and privacy of users.

In this context, the Members of the EDPB and their international colleagues have already adopted a resolution of the ICDPPC, in 2017, on Data Protection in Automated and Connected Vehicles¹. The former WP29 has as well adopted an opinion on the processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS) – Opinion 3/2017²

I have asked for your letter to be transmitted to the relevant EDPB Expert Subgroup dealing with this matter and I can inform you that the work on this topic according to our EDPB work plan 2019/2020 has already started.

We thank you for your continued interest on the work of the EDPB and its forthcoming guidance on this topic.

Yours sincerely,



Andrea Jelinek

¹ <https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-data-protection-in-automated-and-connected-vehicles-.pdf>

² http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47888

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

Opinion of the Board (Art. 64)



Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities

Adopted on 12 March 2019

TABLE OF CONTENTS

1	Summary of the facts	4
2	Legal Context.....	5
2.1	Relevant provisions of the GDPR.....	5
2.2	Relevant provisions of the Framework Directive	6
2.3	Relevant provisions of the ePrivacy Directive	6
3	Scope of this opinion	8
3.1	Matters outside the scope of the GDPR.....	9
3.2	Matters outside the scope of the ePrivacy Directive	9
3.2.1	The general material scope of the ePrivacy Directive.....	9
3.2.2	The extended material scope of articles 5(3) and 13 ePrivacy Directive	11
3.3	Matters within the material scope of both the ePrivacy Directive and the GDPR	11
4	Interplay between the ePrivacy Directive and the GDPR.....	13
4.1	“To particularise”	13
4.2	“To complement”	14
4.3	The meaning of article 95 GDPR.....	14
4.4	Co-existence	15
5	On the competence, tasks and powers of data protection authorities	16
5.1	Enforcement of the GDPR	17
5.2	Enforcement of the ePrivacy Directive.....	18
5.3	Enforcement where GDPR and ePrivacy intersect	19
5.3.1	Question one: are certain processing operations “off limits” for data protection authorities?	19
5.3.2	Question two: Are national ePrivacy provisions “off limits”?	21
6	On the applicability of the cooperation and consistency mechanisms	23
7	Conclusion	24

The European Data Protection Board

Having regard to article 63 and article 64(2) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to article 10 and article 22 of its Rules of Procedure of 25 May 2018, as amended on 23 November 2018,

Whereas:

(1) The main role of the European Data Protection Board (hereafter the Board) is to ensure the consistent application of the Regulation 2016/679 (here after GDPR) throughout the European Economic Area. Article 64(2) GDPR provides that any supervisory authority, the Chair of the Board or the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the Board with a view to obtaining an opinion. The aim of this opinion is to examine a matter of general application or which produces effects in more than one Member State.

(2) On 3 December 2018, the Belgian Data Protection Authority requested the European Data Protection Board to examine and issue an Opinion on the interplay between the GDPR and the ePrivacy Directive, in particular regarding the competence, tasks and powers of data protection authorities.

(3) The opinion of the Board shall be adopted pursuant to article 64(3) GDPR in conjunction with article 10 (2) of the Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. On 3 December 2018, the Belgian DPA requested the European Data Protection Board to examine and issue an opinion on the interplay between the ePrivacy Directive¹ and the GDPR, submitting the following questions :
 - a. Regarding the **competence, tasks and powers** of data protection authorities², whether
 - i. data protection authorities are able or not able to exercise their competence, tasks and powers in relation to processing that triggers, at least in relation to certain processing operations, the material scope of both the GDPR and the ePrivacy Directive; and if so, whether
 - ii. data protection authorities may or should take into account provisions of the ePrivacy Directive and/or its national implementations when exercising their competences, tasks and powers under the GDPR (e.g., when assessing the lawfulness of processing) and if so, to what extent.
 - b. whether the **cooperation and consistency mechanisms** can or should be applied in relation to processing that triggers, at least in relation to certain processing operations, the material scope of both the GDPR and the ePrivacy Directive; and
 - c. the extent to which processing **can be governed by provisions of both** the ePrivacy Directive and the GDPR and whether or not this affects the answers to questions 1 and 2.
2. The Board considers that these questions concern a matter of general application of the GDPR, as there is a clear need for a consistent interpretation among data protection authorities on the boundaries of their competences, tasks and powers. Clarification is particularly needed to ensure, amongst other, a consistent practice of mutual assistance in accordance with article 61 of the GDPR and joint operations in accordance with article 62 of the GDPR.
3. This opinion does not relate to any such division of competences, tasks and powers of data protection authorities under the proposal for the ePrivacy Regulation.

¹ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) as amended by Directive 2006/24/EC and Directive 2009/136/EC.

² As set forth by articles 55-58 GDPR. The term “data protection authorities” (as opposed to “supervisory authorities”) shall be used throughout this Opinion in order to clearly distinguish the “supervisory authorities” envisaged by the GDPR from other types of supervisory authorities, such as the national regulatory authorities mentioned in Directive 2002/58/EC.

2 LEGAL CONTEXT

2.1 Relevant provisions of the GDPR

4. According to article 2(1), the GDPR applies to “*the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.*”

Article 2(2) of the GDPR states that the GDPR shall not apply to the processing of personal data:

- “(a) in the course of an activity which falls outside the scope of Union law;
- “(b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;
- “(c) by a natural person in the course of a purely personal or household activity;
- “(d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security”.

5. Article 5, entitled “Principles relating to the processing of personal data”, contains the principles applicable to any processing of personal data, including the requirement that any processing of personal data shall be lawful and fair.³ Article 6 describes the circumstances in which processing of personal data shall be lawful, one of which relates to the consent of the data subject. Article 7 further specifies the conditions for valid consent within the meaning of the GDPR.⁴
6. Article 51(1) sets forth the legal mandate of data protection authorities, which is to monitor the application of the GDPR in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union. Articles 55, 57 and 58 specify the competences, tasks and powers of each data protection authority. Chapter VII of the GDPR, entitled ‘Cooperation and Consistency’, specifies the different ways in which data protection authorities shall cooperate in order to contribute to a consistent application of the GDPR.
7. Article 94, entitled ‘Repeal of Directive 95/46’, states that

- “1. Directive 95/46/EC is repealed with effect from 25 May 2018.
- 2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.”

³ See also recital (39) GDPR (“Any processing of personal data should be lawful and fair. [...]”).

⁴ See the WP29 Guidelines on consent under Regulation 2016/679, WP259 rev.01, endorsed by the EDPB on 25 May 2018.

8. Article 95, entitled ‘Relationship with Directive 2002/58/EC’, stipulates that

“This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.”

9. Recital (173) of the GDPR stipulates that:

“(173) This Regulation should apply to all matters concerning the protection of fundamental rights and freedoms vis-à-vis the processing of personal data which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC of the European Parliament and of the Council, including the obligations on the controller and the rights of natural persons. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, that Directive should be amended accordingly. Once this Regulation is adopted, Directive 2002/58/EC should be reviewed in particular in order to ensure consistency with this Regulation.”

2.2 Relevant provisions of the Framework Directive

10. Article 2(g) of the Framework Directive⁵ defines a ‘national regulatory authority’ as

“the body or bodies charged by a Member State with any of the regulatory tasks assigned in this Directive and the Specific Directives.”

11. Article 2(l) of the Framework Directive states that

“‘Specific Directives’ means Directive 2002/20/EC (Authorisation Directive), Directive 2002/19/EC (Access Directive), Directive 2002/22/EC (Universal Service Directive) and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).”

12. Article 3(1) of the Framework Directive provides that

“Member States shall ensure that each of the tasks assigned to national regulatory authorities in this Directive and the Specific Directives is undertaken by a competent body.”

2.3 Relevant provisions of the ePrivacy Directive

13. Article 1(2) of the ePrivacy Directive stipulates that

“The provisions of this Directive particularise and complement [Regulation (EU) 2016/679] for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.”⁶

⁵ Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).

⁶ In accordance with article 94(2) of the GDPR, all references to Directive 95/46 in the ePrivacy Directive have been replaced with “[Regulation (EU) 2016/679]” and references to the “Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC” have been replaced with “[European Data Protection Board]”.

14. Article 2(f) of the ePrivacy Directive states that

“consent by a user or subscriber corresponds to the data subject's consent in [Regulation (EU) 2016/679]”

15. Article 15(2) of the ePrivacy Directive stipulates that

“The provisions of [Chapter VIII on remedies, liability and penalties] of [Regulation (EU) 2016/679] shall apply with regard to national provisions adopted pursuant to this Directive and with regard to the individual rights derived from this Directive.”

16. Article 15(3) of the ePrivacy Directive stipulates that

“The [European Data Protection Board] shall also carry out the tasks laid down in [Article 70 of Regulation (EU) 2016/679] with regard to matters covered by this Directive, namely the protection of fundamental rights and freedoms and of legitimate interests in the electronic communications sector.”

17. Article 15a, entitled 'Implementation and enforcement', stipulates that

“1. Member States shall lay down the rules on penalties, including criminal sanctions where appropriate, applicable to infringements of the national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. [...]”

“2. Without prejudice to any judicial remedy which might be available, Member States shall ensure that the competent national authority and, where relevant, other national bodies have the power to order the cessation of the infringements referred to in paragraph 1.”

“3. Member States shall ensure that the competent national authority and, where relevant, other national bodies have the necessary investigative powers and resources, including the power to obtain any relevant information they might need to monitor and enforce national provisions adopted pursuant to this Directive.”

“4. The relevant national regulatory authorities may adopt measures to ensure effective cross-border cooperation in the enforcement of the national laws adopted pursuant to this Directive and to create harmonised conditions for the provision of services involving cross-border data flows.”

“The national regulatory authorities shall provide the Commission, in good time before adopting any such measures, with a summary of the grounds for action, the envisaged measures and the proposed course of action. The Commission may, having examined such information and consulted ENISA and the [European Data Protection Board], make comments or recommendations thereupon, in particular to ensure that the envisaged measures do not adversely affect the functioning of the internal market. National regulatory authorities shall take the utmost account of the Commission's comments or recommendations when deciding on the measures.”

18. Recital (10) of the ePrivacy Directive states that

“In the electronic communications sector, [Regulation (EU) 2016/679] applies in particular to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this Directive, including the obligations on the controller and the rights of individuals. [Regulation (EU) 2016/679] applies to non-public communications services.”

3 SCOPE OF THIS OPINION

19. The GDPR has the objective to protect fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union.⁷ To achieve this objective, the GDPR lays down common rules on data processing, so as to ensure consistent effective protection of personal data throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market. The rules serve to ensure a balance between the (potential) benefits of data processing and the (potential) drawbacks.
20. The ePrivacy Directive has the objective to harmonise the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.⁸ The ePrivacy Directive seeks therefore to ensure respect for the rights set out in articles 7 and 8 of the Charter. In this regard, the ePrivacy Directive aims to “particularise and complement” the provisions of the GDPR, with respect to the processing of personal data in the electronic communication sector.⁹
21. The questions referred to the Board are limited to processing that triggers the material scope of both the GDPR and the ePrivacy Directive. In order to further clarify the scope of this opinion, the following sections clarify:
 - where there is no interplay between the GDPR and the ePrivacy Directive because the matter falls outside of the scope of the GDPR;
 - where there is no interplay between the GDPR and the ePrivacy Directive because the matter falls outside of the scope of the ePrivacy Directive; and
 - where there is an interplay between the GDPR and the ePrivacy Directive because the processing triggers the material scope of both the GDPR and the ePrivacy Directive.

⁷ Article 1 of the GDPR.

⁸ Article 1(1) of the ePrivacy Directive.

⁹ Article 1(1)-(2) of the ePrivacy Directive, to be read in light of article 94(2) GDPR.

3.1 Matters outside the scope of the GDPR

22. In principle, the material scope of the GDPR covers any form of processing of personal data, regardless of the technology used.¹⁰ The GDPR shall not be applicable when:
- no personal data are being processed (e.g. a phone number of an automated customer service of a legal person, or the IP address of a digital photocopier in a corporate network do not constitute personal data);
 - the activities fall outside of the material scope of the GDPR, taking into account article 2(2) and (3) GDPR; or
 - the activities fall outside the territorial scope of the GDPR.¹¹

3.2 Matters outside the scope of the ePrivacy Directive

23. A particularity of the ePrivacy Directive is that two of its provisions have a wider scope of application than the other provisions, for which the scope of application is limited to the provision of publicly available electronic communications services in public communications networks. Consequently, as outlined in the following sections, two questions need to be answered to determine whether an activity falls inside or outside the material scope of the ePrivacy Directive.

3.2.1 The general material scope of the ePrivacy Directive

24. According to its article 3, the ePrivacy Directive applies to "*the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices*".
25. As such, the ePrivacy Directive in first instance addresses publicly available electronic communication services and electronic communication networks.¹²
The Electronic Communications Code¹³ provides that services which are functionally equivalent to electronic communications services are covered.

¹⁰ See also recital (46) of the ePrivacy Directive.

¹¹ Article 3 GDPR. See EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), 16 November 2018.

¹² Commission Staff Working Document, Ex-post REFIT evaluation of the ePrivacy Directive 2002/58/EC, COM SWD(2017)005 report, p. 20 ; Report to the Commission "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation", SMART 2013/0071, p. 24 ff.

¹³ Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.

26. For purposes of its general material scope, the ePrivacy Directive applies when each of the following conditions are met:
- there is an electronic communications service (ECS)¹⁴;
 - this service is offered over an electronic communications network¹⁵;
 - the service and network are publicly available¹⁶;
 - the service and network are offered in the EU.
27. Activities which do not meet all of the above criteria are generally out of scope of the ePrivacy Directive.

Examples:

A corporate network which is accessible only to employees for professional purposes does not constitute a “publicly available” electronic communications service. As a result, the transmission of location data via such a network does not fall inside the material scope of the ePrivacy Directive¹⁷

A clock synchronisation service sends a signal over an electronic communications network to all clocks which adhere to its synchronisation protocol (undetermined number of recipients). This service is a broadcast service instead of a communication service in the current context and would also fall outside the material scope of the ePrivacy Directive.

¹⁴ Article 2(d) ePrivacy Directive specifies that ‘communication’ means “any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service” and excludes broadcasting services which may - in theory - reach an unlimited audience. The term ‘electronic communications service’ is currently defined by article 2(d) Framework Directive, though with effect from 21 December 2020 it shall be defined by article 2(4) of the Electronic Communications Code.

¹⁵ ‘Electronic communications network’ is currently defined by article 2(a) Framework Directive, though with effect from 21 December 2020 it shall be defined by article 2(1) of the Electronic Communications Code.

¹⁶ A service for the public is a service available to all members of the public on the same basis, and not only publicly owned services. Compare: EDPS, Opinion 5/2016, Preliminary EDPS Opinion on the review of the ePrivacy Directive (2002/58/EC), p. 12 and Communication by the Commission to the European Parliament and the Council on the status and implementation of Directive 90/388/EEC on competition in the markets for telecommunications services, COM(95) 113 final, 04.04.1995, p. 14.

¹⁷ Commission Staff Working Document, Ex-post REFIT evaluation of the ePrivacy Directive 2002/58/EC, COM SWD(2017)005 report, p. 21 ,

<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017SC0005&from=EN>; Report to the Commission “ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation”, SMART 2013/0071, p. 14,

<https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data>.

3.2.2 The extended material scope of articles 5(3) and 13 ePrivacy Directive

28. The overarching aim of the ePrivacy Directive is to ensure the protection of fundamental rights and freedoms of the public when they make use of electronic communication networks.¹⁸ In light of this aim, articles 5(3) and 13 of the ePrivacy Directive apply to providers of electronic communication services as well as website operators (e.g. for cookies) or other businesses (e.g. for direct marketing).¹⁹

Examples:

Search engine services which store or access cookies on the device of a user fall within the extended material scope of article 5(3) ePrivacy Directive.²⁰

Unsolicited electronic mail sent by a website operator for the purposes of direct marketing also fall within the extended material scope of article 13 ePrivacy Directive.²¹

3.3 Matters within the material scope of both the ePrivacy Directive and the GDPR

29. There are many examples of processing activities which trigger the material scope of both the ePrivacy Directive and the GDPR. A clear example is the use of cookies. In its opinion on online behavioral advertising, the Article 29 Working Party stated that

“If as a result of placing and retrieving information through the cookie or similar device, the information collected can be considered personal data then, in addition to Article 5(3), Directive 95/46/EC will also apply.”²²

30. Case law of the Court of Justice of the European Union (CJEU) confirms that it is possible for processing to fall within the material scope of both the ePrivacy Directive and the GDPR at the same time. In *Wirtschaftsakademie*²³, the CJEU applied Directive 95/46/EC notwithstanding the fact that the underlying processing also involved processing operations falling into the material scope of the ePrivacy Directive. In the pending *Fashion ID* case, the Advocate General expressed the view that both set of rules may be applicable in a case involving social plug-ins and cookies.²⁴
31. Whilst the GDPR replaced Directive 95/46/EC on 25 May 2018, the analysis undertaken by the CJEU and the Article 29 Working Party according to which both legal acts may apply at the same time are

¹⁸ Article 1(1) ePrivacy Directive provides: “This Directive provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.”

¹⁹ Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising, 22 June 2010, WP 171, section 3.2.1 p. 9. Opinion 1/2008 on data protection issues related to search engines (WP148), section 4.1.3, p. 12. ; Report to the Commission “ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation”, SMART 2013/0071, p. 9.

²⁰ Opinion 1/2008 on data protection issues related to search engines (WP148), section 4.1.3, p. 12

²¹ Opinion 1/2008 on data protection issues related to search engines (WP148), section 4.1.3, p. 12.

²² Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising, 22 June 2010, WP 171, p. 9. See also Opinion 1/2008 on data protection issues related to search engines (WP148), section 4.1.3, p. 12-139.

²³ CJEU, C-210/16, 5 June 2018, C-210/16, ECLI:EU:C:2018:388. See in particular paragraphs 33-34.

²⁴ Opinion of Advocate General Bobek in *Fashion ID*, C-40/17, 19 December 2018, ECLI:EU:C:2018:1039. See in particular paragraphs 111-115.

relevant. Recital (30) of the GDPR elaborates on the definition of “online identifiers” in a way that supports the interpretation that processing of personal data may trigger the material scope of both the GDPR and the ePrivacy Directive:

“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.”

32. Worth noting in particular is that ‘IP addresses’ and ‘cookie identifiers’ are mentioned in recital (30), which states that IP addresses and cookie identifiers might be combined with other “unique identifiers” and other information received by the servers to create profiles of natural persons.
33. In other words, the GDPR itself explicitly refers, when clarifying its own material scope (the concept of personal data), to processing activities which also trigger, at least in part, the material scope of the ePrivacy Directive.
34. Another example of an activity which triggers the material scope of both the ePrivacy Directive and the GDPR is the customer relationship between electronic communications service providers and natural person that is a user of its services, which involves personal data processing about customers on the one hand, and are also governed by specific rules for instance on subscriber directories, itemised billing, calling line identification. Traffic data and location data generated by electronic communications services may also involve personal data processing, insofar as they relate to natural persons.
35. Finally, article 95 of the GDPR and recital (173) GDPR confirm the lex generalis-lex specialis relationship between the GDPR and the ePrivacy Directive, with article 95 providing that the GDPR shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the EU in relation to matters for which they are subject to specific obligations with the same objective set out in the ePrivacy Directive.

36. This opinion aims to provide clarity on the competence, tasks and powers of data protection authorities, with regards to cases which trigger the material scope of both the ePrivacy Directive and the GDPR as briefly laid out in the previous sections. The following sections describe some instances of interplay between the provisions of the ePrivacy Directive and the GDPR and how each sets of rules relate to one and other.

4 INTERPLAY BETWEEN THE EPRIVACY DIRECTIVE AND THE GDPR

37. Although an overlap in material scope exists between the ePrivacy Directive and the GDPR, this does not necessarily lead to a conflict between the rules. Besides this becoming apparent from reading the various provisions side by side, article 1(2) of the ePrivacy Directive expressly provides that "*the provisions of this Directive particularise and complement Directive 95/46/EC (...)*"²⁵. To properly understand the interplay between the ePrivacy Directive and the GDPR, it is necessary to first clarify the meaning of article 1(2) of the ePrivacy Directive. After that, the meaning and implications of article 95 GDPR shall be clarified.

4.1 "To particularise"

38. A number of provisions of the ePrivacy Directive "*particularise*" the provisions of the GDPR with respect to the processing of personal data in the electronic communication sector. In accordance with the principle *lex specialis derogate legi generali*, special provisions prevail over general rules in situations which they specifically seek to regulate.²⁶ In situations where the ePrivacy Directive "particularises" (i.e. renders more specific) the rules of the GDPR, the (specific) provisions of the ePrivacy Directive shall, as "*lex specialis*", take precedence over the (more general) provisions of the GDPR.²⁷ However, any processing of personal data which is not specifically governed by the ePrivacy Directive (or for which the ePrivacy Directive does not contain a "special rule"), remains subject to the provisions of the GDPR.
39. One example of where the ePrivacy Directive "particularises" the provisions of the GDPR can be found in article 6 of the ePrivacy Directive, which concerns the processing of so-called "traffic data". Ordinarily speaking, the processing of personal data can be justified on the basis of each of the lawful grounds mentioned in article 6 GDPR. However, the full range of possible lawful grounds provided by article 6 GDPR cannot be applied by the provider of an electronic communications service to processing of traffic data, because article 6 ePrivacy Directive explicitly limits the conditions in which traffic data, including personal data, may be processed. In this case, the more specific provisions of the ePrivacy Directive must take precedence over the more general provisions of the GDPR. Article 6 of the ePrivacy Directive does not however, curtail the applications of other provisions of the GDPR, such as the rights of the data subject. Nor does it negate the requirement that processing of personal data must be lawful and fair (article 5(1)a GDPR).
40. A similar situation occurs with regards article 5(3) of the ePrivacy Directive, insofar as the information stored in the end-user's device constitutes personal data. Article 5(3) of the ePrivacy Directive provides that, as a rule, prior consent is required for the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user.²⁸ To the extent that the

²⁵ Article 94.2 GDPR provides that references to the repealed Directive 95/46 shall be construed as references to the GDPR.

²⁶ Judgement of the CJEU in Joined Cases T-60/06 RENV II and T-62/06 RENV II, 22 April 2016, ECLI:EU:T:2016:233, at paragraph 81.

²⁷ Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising, 22 June 2010, WP 171, p. 10.

²⁸ Pursuant to article 5(3) information in the terminal equipment of a subscriber or user may also be stored or accessed insofar as its consists of technical storage or access for the sole purpose of carrying out the transmission

information stored in the end-users device constitutes personal data, article 5(3) of the ePrivacy Directive shall take precedence over article 6 of the GDPR with regards to the activity of storing or gaining access to this information. The outcome is similar in the interplay between article 6 of the GDPR and articles 9 and 13 of the ePrivacy Directive. Where these articles require consent for the specific actions they describe, the controller cannot rely on the full range of possible lawful grounds provided by article 6 of the GDPR.

41. A corollary of the “*lex specialis*” principle is that there shall only be a derogation from the general rule insofar as the law governing a specific subject matter contains a special rule. The facts of the case must be carefully analysed to find how far the derogation extends, especially in cases where data undergoes many different kinds of processing - either in parallel or sequentially.

Example:

A data broker engages in profiling on the basis of information concerning the internet browsing behaviour of individuals, collected by the use of cookies, but which may also include personal data obtained via other sources (e.g. “commercial partners”). In such a case, a subset of the processing in question, namely the placing or reading of cookies must comply with the national provision transposing article 5(3) of the ePrivacy Directive. Subsequent processing of personal data including personal data obtained by cookies must also have a legal basis under article 6 of the GDPR in order to be lawful.²⁹

4.2 “To complement”

42. The ePrivacy Directive also contains provisions that “*complement*” the provisions of the GDPR with respect to the processing of personal data in the electronic communication sector. For example, several of the provisions of the ePrivacy Directive seeks to protect “subscribers” and “users” of a publicly available electronic communications service. Subscribers of a publicly available electronic communications service may be natural or legal persons. By supplementing the GDPR, the ePrivacy Directive protects not only the fundamental rights of natural persons and particularly their right to privacy, but also the legitimate interests of legal persons.³⁰

4.3 The meaning of article 95 GDPR

43. Article 95 of the GDPR stipulates that the GDPR “*should not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.*” (emphasis added).

of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.

²⁹ While data protection authorities cannot enforce article 5(3) of the ePrivacy Directive (unless national law confers this competence to them), they should take into account that the processing as a whole involves specific activities for which the EU legislature has sought to provide additional protection in order to avoid undermining this protection.

³⁰ Recital (12) of the ePrivacy Directive.

44. The aim of article 95 GDPR is therefore to avoid the imposition of unnecessary administrative burdens upon controllers who would otherwise be subject to similar but not quite identical administrative burdens. An example that illustrates the application of this article relates to the personal data breach notification obligation, which is imposed by both the ePrivacy Directive³¹ and the GDPR³². They both provide for an obligation to ensure security, as well as an obligation to notify personal data breaches to the competent national authority and the data protection authority, respectively. These obligations are applicable in parallel under the two different pieces of legislation, according to their respective scopes of application. Clearly, an obligation to notify under both acts, once in compliance with the GDPR and once in compliance with national ePrivacy legislation would constitute an added burden without immediate apparent benefits for data protection. Following article 95 of the GDPR, the electronic communications service providers who have notified a personal data breach in compliance with applicable national ePrivacy legislation are not required to separately notify data protection authorities of the same breach pursuant to article 33 of the GDPR.

4.4 Co-existence

45. Where specific provisions exist which govern a particular processing operation or set of operations, the specific provisions should be applied (*lex specialis*), in all other cases (i.e. where no specific provisions govern a particular processing operation or set of operations), the general rule will apply (*lex generalis*).
46. Recital (173) confirms that, in respect of the processing of personal data to which the specific obligations of the ePrivacy Directive do not apply, the GDPR shall remain applicable:

*“to all matters concerning the protection of fundamental rights and freedoms vis-à-vis the processing of personal data which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC of the European Parliament and of the Council, including the obligations on the controller and the rights of natural persons”.*³³

47. Recital (173) to the GDPR reiterates that, which is already stated in recital (10) to the ePrivacy Directive, which provides that: *“In the electronic communications sector, [Regulation (EU) 2016/679] applies in particular to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this Directive, including the obligations on the controller and the rights of individuals.”*
48. For example, a provider of a public communications network or publicly available electronic communications service must comply with national rules transposing article 6(2) of the ePrivacy Directive concerning traffic data when processing data necessary for the purposes of subscriber billing and interconnection payments. Due to the absence of specific ePrivacy provisions on, for example, the right of access, the provisions of the GDPR apply. Likewise, recital (32) of the ePrivacy Directive confirms that where the provider of an electronic communications service or of a value added service

³¹ Article 4 ePrivacy Directive.

³² Articles 32-34 GDPR.

³³ Recital (173) goes on to state that “In order to clarify the relationship between this Regulation and Directive 2002/58/EC, that Directive should be amended accordingly. Once this Regulation is adopted, Directive 2002/58/EC should be reviewed in particular in order to ensure consistency with this Regulation.” That review process is still ongoing.

subcontracts the processing of personal data necessary for the provision of these services to another entity, such subcontracting and subsequent data processing should be in full compliance with the requirements regarding controllers and processors of personal data as set out in the GDPR.

49. The previous sections described how the provisions of the ePrivacy Directive and the GDPR interact in case of processing which triggers the material scope of application of both instruments. The following sections turn to the resolving the questions referred to the Board regarding the competence, tasks and powers of data protection authorities, with regards to cases which at least in part fall within the scope of the ePrivacy Directive.

5 ON THE COMPETENCE, TASKS AND POWERS OF DATA PROTECTION AUTHORITIES

50. The Belgian SA referred two questions concerning the competence, tasks and powers of data protection authorities – as set out by articles 55-58 of the GDPR – to the Board, which can be paraphrased as follows:
 - Does the mere fact that the processing of personal data triggers the material scope of both the GDPR and the ePrivacy Directive, limit the competences, tasks and powers of data protection authorities under the GDPR? In other words, is there a subset of data processing operations that should be excluded from their consideration, and if so to what extent?
 - When exercising their competences, tasks and powers under the GDPR, should data protection authorities take into account the provisions of the ePrivacy Directive (e.g., when assessing the lawfulness of processing), and if so to what extent? In other words, should infringements of national ePrivacy rules be taken into account or set aside when assessing compliance with the GDPR, and if so, under which circumstances?
51. As a preliminary matter, it should be noted that Member States are required to ensure full effectiveness of EU law, notably by providing for appropriate enforcement mechanisms. This obligation is founded on the principle of sincere cooperation established in article 4(3) TFEU.³⁴ The following sections describe in brief the enforcement provisions of the GDPR and ePrivacy Directive respectively and the interplay between them.

³⁴ Article 4.3 TEU provides: “*Pursuant to the principle of sincere cooperation, the Union and the Member States shall, in full mutual respect, assist each other in carrying out tasks which flow from the Treaties. The Member States shall take any appropriate measure, general or particular, to ensure fulfilment of the obligations arising out of the Treaties or resulting from the acts of the institutions of the Union. The Member States shall facilitate the achievement of the Union's tasks and refrain from any measure which could jeopardise the attainment of the Union's objectives.*”

5.1 Enforcement of the GDPR

52. The GDPR provides for enforcement of its provisions by independent data protection authorities. In this regard, it should also be noted that article 8 of the Charter of Fundamental Rights of the EU (the Charter) provides that the processing of personal data shall be subject to control by an independent authority:

"Article 8 – Protection of personal data

- 1. Everyone has the right to the protection of personal data concerning him or her.*
- 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
- 3. Compliance with these rules shall be subject to control by an independent authority."*

53. Data protection authorities are given a legal mandate in this regard, as set forth in article 51(1) GDPR, which is to monitor the application of the GDPR in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union.
54. The GDPR contains one exception and one possibility to derogate this mandate:

- the competence of the supervisory authorities shall not cover the processing of personal data when courts are acting in their judicial capacity (article 55(3) GDPR);
- for processing carried out for journalistic purposes or for the purpose of academic, artistic or literary expression, Member States may provide for exemptions and derogations from amongst others Chapters VI (independent supervisory authorities) and VII (cooperation and consistency) of the GDPR (article 85 GDPR);

In addition, the powers of the data protection authorities may be extended in line with article 58(6) GDPR and may in particular grant the power to fine public authorities and bodies, should a Member State provide so in the national legislation (article 83(7) GDPR).

Being exceptions to the general rule, these provisions must be narrowly construed.

55. Where the GDPR limits or allows for derogations on the competences, tasks and powers of data protection authorities, it has done so explicitly. The GDPR also does not exclude data protection authorities in any way from exercising their competences, tasks and powers in relation to processing to the extent it triggers the material scope of the GDPR. The question therefore becomes whether the EU legislature has envisaged or allowed a derogation on the general competence of data protection authorities in cases where provisions of the ePrivacy Directive apply to the processing at issue.

5.2 Enforcement of the ePrivacy Directive

56. The enforcement of the provisions of the ePrivacy Directive is closely linked to the Framework Directive³⁵, which stipulates in article 3(1) that “*Member States shall ensure that each of the tasks assigned to national regulatory authorities in this Directive and the Specific Directives is undertaken by a competent body*³⁶.³⁶”
57. Article 2(g) of the Framework Directive defines a ‘national regulatory authority’ as
“the body or bodies charged by a Member State with any of the regulatory tasks assigned in this Directive and the Specific Directives.”
58. Member states have chosen different ways of allocating the task of enforcing national ePrivacy rules to one or more entities.³⁷ This level of variation is possible, as the ePrivacy Directive only sets out some general goals to be achieved by the member states on this matter.
59. The ePrivacy Directive does not state that only one national body shall be competent to enforce its provisions. In fact, article 15a of the ePrivacy Directive explicitly provides that more than one national body may be competent to enforce its provisions. Article 15a also provides for the implementation and enforcement of the Directive by Member States including the obligations that Member States shall lay down rules on penalties, grant power to order cessation of infringements, grant investigative powers and resources etc. as follows:
- “1. *Member States shall lay down the rules on penalties, including criminal sanctions where appropriate, applicable to infringements of the national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for must be effective, proportionate and dissuasive and may be applied to cover the period of any breach, even where the breach has subsequently been rectified. The Member States shall notify those provisions to the Commission by 25 May 2011, and shall notify it without delay of any subsequent amendment affecting them.*
2. *Without prejudice to any judicial remedy which might be available, Member States shall ensure that the competent national authority and, where relevant, other national bodies have the power to order the cessation of the infringements referred to in paragraph 1.*
3. *Member States shall ensure that the competent national authority and, where relevant, other national bodies have the necessary investigative powers and resources, including the power to obtain any relevant information they might need to monitor and enforce national provisions adopted pursuant to this Directive.*
4. *The relevant national regulatory authorities may adopt measures to ensure effective cross-border cooperation in the enforcement of the national laws adopted pursuant to this Directive*

³⁵ Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), as amended.

³⁶ Article 2(l) of the Framework Directive clarifies that “‘Specific Directives’ refers to Directive 2002/20/EC (Authorisation Directive), Directive 2002/19/EC (Access Directive), Directive 2002/22/EC (Universal Service Directive) and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).”

³⁷ Report to the Commission “ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation”, SMART 2013/0071, p. 33 ff.

and to create harmonised conditions for the provision of services involving cross-border data flows.”

60. In addition article 15(2) of the ePrivacy Directive contains a provision referring to the provisions of Directive 95/46/EC on judicial remedies, liability and sanctions, now to be read as a reference to the GDPR:

“The provisions of Chapter III on judicial remedies, liability and sanctions of Directive 95/46/EC shall apply with regard to national provisions adopted pursuant to this Directive and with regard to the individual rights derived from this Directive.”

61. Article 15(3) of the ePrivacy Directive also provides:

“The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC shall also carry out the tasks laid down in Article 30 of that Directive with regard to matters covered by this Directive, namely the protection of fundamental rights and freedoms and of legitimate interests in the electronic communications sector.”³⁸

5.3 Enforcement where GDPR and ePrivacy intersect

62. The ePrivacy Directive particularises and complements the GDPR and moreover refers to the latter’s provisions on judicial remedies, liability and sanctions (article 15(2) of the ePrivacy Directive read in light of article 94 of the GDPR)..

5.3.1 Question one: are certain processing operations “off limits” for data protection authorities?

- *Does the mere fact that the processing of personal data triggers the material scope of both the GDPR and the ePrivacy Directive, limit the competences, tasks and powers of data protection authorities under the GDPR? In other words, is there a subset of processing operations they should exclude from their consideration, and if so which processing operations shall be excluded?*
63. Under the GDPR, Member States must have appointed one or more supervisory authorities. Member States may have appointed the same authority to be competent for (part of) the enforcement of the national implementation of the ePrivacy Directive, but may also have opted for one or more other authorities, for example a national telecommunications regulatory authority (NRA), a consumer protection organisation, or a ministry.

³⁸ Art. 15(3) of the ePrivacy directive provides “*The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC shall also carry out the tasks laid down in Article 30 of that Directive with regard to matters covered by this Directive, namely the protection of fundamental rights and freedoms and of legitimate interests in the electronic communications sector.*”

Article 94.2 GDPR provides that “*References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.*”

Consequently, Article 30 of Directive 95/46 shall be construed as a reference to the relevant sections of article 70 GDPR (Tasks of the Board).

64. The ePrivacy Directive gives Member States flexibility on which authority or body to entrust with enforcement of its provisions.
65. While the ePrivacy Directive refers to the provisions of the GDPR regarding judicial remedies, liability and sanctions (article 15(2) of the ePrivacy Directive), article 15a(1) of the ePrivacy Directive details the “Implementation and enforcement” provisions of the ePrivacy Directive. For example, article 15a(1) provides that *“Member States shall lay down the rules on penalties, including criminal sanctions where appropriate, applicable to infringements of the national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented...”*. As such, the ePrivacy Directive explicitly provides Member States discretion with respect to penalties and article 15(2) does not interfere with the discretion offered to the Member States on enforcement (i.e., to determine who enforces the provisions of the ePrivacy Directive).³⁹
66. In case national law confers competence for the enforcement of the ePrivacy Directive on the data protection authority, the law should also determine the tasks and powers of the data protection authority in relation to the enforcement of the ePrivacy Directive. The data protection authority cannot automatically rely on the tasks and powers foreseen in the GDPR to take action to enforce national ePrivacy rules, as these GDPR tasks and powers are tied to the enforcement of the GDPR. National law may assign tasks and powers inspired by the GDPR, but may also grant other tasks and powers to the data protection authority for enforcement of national ePrivacy rules in accordance with article 15a of the ePrivacy Directive.
67. Discretion exists only within the requirements and limits set forth in higher rules. Article 8(3) of the Charter demands that compliance with personal data protection rules is subject to control by an independent authority.⁴⁰
68. When the processing of personal data triggers the material scope of both the GDPR and the ePrivacy Directive, data protection authorities are competent to scrutinize subsets of the processing which are governed by national rules transposing the ePrivacy Directive only if national law confers this competence on them. However, the competence of data protection authorities under the GDPR in any event remains unabridged as regards processing operations which are not subject to special rules contained in the ePrivacy Directive. This demarcation line may not be modified by national law transposing the ePrivacy Directive (e.g. by broadening the material scope beyond what is required by the ePrivacy Directive and granting exclusive competence for that provision to the national regulatory authority).
69. Data protection authorities are competent to enforce the GDPR. The mere fact that a subset of the processing falls within the scope of the ePrivacy directive, does not limit the competence of data protection authorities under the GDPR.

³⁹ Note that Article 15a(1) of the ePrivacy Directive was introduced by 2009/136/EC (i.e. an amendment to the ePrivacy Directive).

⁴⁰ The case law of the CJEU concerning article 28 of Directive 95/46 has clarified the requirements as regards independence: see e.g. Judgement of 9 March 2010, C-518/07 (Commission v. Germany), paragraph 17 and following; Judgment 16 October 2012, C-614/10 (Commission v. Austria), par. 36 and following; Judgment of 6 October 2015, C-362/14 (Safe Harbour), par. 41 and following; Judgment of 21 December 2016, C-203/15 and C-698/15 (Tele2/Watson), par. 123.

70. Where exclusive competence has been given to a body other than the data protection authority, national procedural law determines what should happen when data subjects nevertheless lodge complaints with the data protection authority regarding for instance the processing of personal data in the form of traffic or location data, unsolicited electronic communications or the collection of personal data by use of cookies without also complaining about a (potential) infringement of the GDPR.

5.3.2 Question two: Are national ePrivacy provisions “off limits”?

- *When exercising their competences, tasks and powers under the GDPR, should data protection authorities take into account the provisions of the ePrivacy Directive (e.g., when assessing the lawfulness of processing), and if so to what extent? In other words, should infringements of national ePrivacy rules be taken into account or set aside when in assessing compliance with the GDPR, and if so, under which circumstances?*
71. An example illustrates the difference with question one. Consider a data broker, who engages in profiling on the basis of information obtained from two distinct sources. The first source is data collected concerning the internet browsing behaviour of individuals, through the use of cookie identifiers and/or other device identifiers. The second source is data obtained via commercial partners, who share data about participants in prize draws or cash-back programs.
72. Profiling of individuals on the basis of personal data generally falls within the scope of the GDPR and therefore within the competence of data protection authorities. If a data protection authority receives a complaint regarding the profiling activities undertaken by the data broker, what consideration may data protection authorities give to specific rules, in this case national ePrivacy rules, when assessing compliance with the GDPR?
73. Worth noting is that ePrivacy Directive is a specific example of a law which offers special protection to particular categories of data which may be personal data. Other legal texts also offer particular protection to specific kinds of data which may be personal data for various reasons (e.g. the context of the processing, the nature of the data or the risks for data subjects).⁴¹
74. Member States are obligated to appoint one or more authorities to supervise compliance with the national law transposing the ePrivacy Directive, and such authority(-ies) is then responsible for enforcement of this law. The national law transposing the ePrivacy Directive applies to the specific processing operation(s) governed by the ePrivacy Directive (e.g. a processing operation which consists of the storing of or access to information stored on the end-users device).

⁴¹ An example can be found in the financial sector: Specific protection is afforded to data used to assess a person’s creditworthiness or the publicity to be given to administrative penalties. See: Article 21(1) in Directive 2014/17/EU of the European Parliament and of the Council of 4 February 2014 on credit agreements for consumers relating to residential immovable property and amending Directives 2008/48/EC and 2013/36/EU and Regulation (EU) No 1093/2010; Articles 68-69 in Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC.

Another example can be found in the rules on clinical trials: see articles 28 - 35 of Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC.

75. Unless national law gives them such competence, data protection authorities cannot enforce the provisions (of national law implementing) the ePrivacy Directive as such when exercising their competences under the GDPR. However, as indicated earlier, the processing of personal data which involves operations subject to the material scope of the ePrivacy Directive, may involve additional aspects for which the ePrivacy Directive does not contain a “special rule”. For example, article 5(3) of the ePrivacy Directive contains a special rule for the storing of information, or the gaining of access to information already stored, in the terminal device of an end-user. It does not contain a special rule for any prior or subsequent processing activities (e.g., the storage and analysis of data regarding web browsing activity for purposes of online behavioural advertising or security purposes). As a result, data protection authorities remain fully competent to assess the lawfulness of all other processing operations that follow the storing of or access to information in the terminal device of the end-user.⁴²
76. An infringement of the GDPR might also constitute an infringement of national ePrivacy rules. The data protection authority may take this factual finding as to an infringement of ePrivacy rules into consideration when applying the GDPR (e.g., when assessing compliance with the lawfulness or fairness principle under article 5(1)a GDPR). However, any enforcement decision must be justified on the basis of the GDPR, unless the data protection authority has been granted additional competences by Member State law.
77. If national law designates the data protection authority as competent authority under the ePrivacy Directive, this data protection authority has the competence to directly enforce national ePrivacy rules in addition to the GDPR (otherwise it does not).
78. As a general comment, where several authorities are competent for the different legal instruments, they should ensure that enforcement of both instruments is consistent inter alia to avoid a breach of the non bis in idem principle in case infringements of provisions of the GDPR and ePrivacy Directive which took place in the context of one processing activity are strongly linked.

⁴² In this regard, reference should be made to the Opinion of the WP29 on legitimate interest (06/2014) and the WP29 opinion on purpose limitation (Opinion 03/2013), which clarify that certain forms of behavioural advertising require consent of the data subject, not just because of article 5(3). Opinion on purpose limitation states:

“The second potential scenario is when an organisation specifically wants to analyse or predict the personal preferences, behaviour and attitudes of individual customers, which will subsequently inform ‘measures or decisions’ that are taken with regard to those customers. In these cases, free, specific, informed and unambiguous ‘opt-in’ consent would almost always be required, otherwise further use cannot be considered compatible. Importantly, such consent should be required, for example, for tracking and profiling for purposes of direct marketing, behavioural advertisement, data-brokering, location-based advertising or tracking-based digital market research.”

Opinion on legitimate interests states:

“Instead of merely offering the possibility to opt out of this type of profiling and targeted advertisement, an informed consent would be necessary, pursuant to Article 7(a) but also under Article 5(3) of the ePrivacy Directive. As a consequence, Article 7(f) should not be relied on as a legal ground for the processing.”

6 ON THE APPLICABILITY OF THE COOPERATION AND CONSISTENCY MECHANISMS

79. The third question submitted by the Belgian Data Protection Authority to the Board can paraphrased as follows:
- *to what extent is the cooperation and consistency mechanisms applicable in relation to processing that triggers, at least in relation to certain processing operations, the material scope of both the GDPR and the ePrivacy Directive?*
80. Following Chapter VII of the GDPR, the cooperation and consistency mechanisms available to data protection authorities under the GDPR concern the monitoring of the application of GDPR provisions. The GDPR mechanisms do not apply to the enforcement of the provisions contained in the ePrivacy Directive as such.
81. In any event, article 15(3) of the ePrivacy Directive provides:
- "The [European Data Protection Board] shall also carry out the tasks laid down in [article 70 of Regulation (EU) 2016/679] with regard to matters covered by this Directive, namely the protection of fundamental rights and freedoms and of legitimate interests in the electronic communications sector."*
82. Regarding cooperation between authorities competent for the enforcement of the ePrivacy Directive, article 15a(4) of the ePrivacy Directive provides that "*the relevant national regulatory authorities may adopt measures to ensure effective cross-border cooperation in the enforcement of the national laws adopted pursuant to this Directive and to create harmonised conditions for the provision of services involving cross- border data flows (...).*"
83. Such cross-border cooperation between authorities competent for the enforcement of the ePrivacy Directive, including data protection authorities, national regulatory authorities and other authorities, may take place to the extent that relevant national regulatory authorities adopt measures to allow such cooperation.
84. It should be noted that the cooperation and consistency mechanism remains fully applicable, however, insofar as the processing is subject to the general provisions of the GDPR (and not to a "special rule" contained in the ePrivacy Directive). For example, even if the processing of personal data (e.g. profiling) in part relies on access to information stored in the end-user's device, the data protection rules which are not provided by the ePrivacy Directive (e.g. data subject rights, principles of processing) for any processing of personal data that takes place following the access to information stored in the end-user's device shall be subject to the provisions of the GDPR, including the cooperation and consistency mechanisms..
85. In practice, data protection authorities will have carefully select which 'line of communication' to use, especially if they are not only enforcing the GDPR but also competent to enforce (part of) the national transposition of the ePrivacy Directive. The default 'line of communication' - as detailed in Chapter VII (Cooperation and Consistency) of the GDPR - shall be used for any and all parts of a procedure that envisage using the enforcement powers granted by the GDPR in response to an infringement of the GDPR.

The discretionary ‘line of communication’ may be used by data protection authorities in the context of their distinct enforcement powers granted by the national transposition of the ePrivacy Directive and only insofar as the procedure aims to respond to infringements of national ePrivacy rules governing the specific behaviours regulated by the ePrivacy Directive. As soon as it concerns matters falling within the scope of the GDPR, data protection authorities are obliged to apply the cooperation and consistency mechanism provided by the GDPR.

7 CONCLUSION

- *Does the mere fact that the processing of personal data triggers the material scope of both the GDPR and the ePrivacy Directive, limit the competences, tasks and powers of data protection authorities under the GDPR? In other words, is there a subset of data processing operations they should set aside, and if so when?*
- 86. When the processing of personal data triggers the material scope of both the GDPR and the ePrivacy Directive, data protection authorities are competent to scrutinize the data processing operations which are governed by national ePrivacy rules only if national law confers this competence on them, and such scrutiny must happen within the supervisory powers assigned to the authority by the national law transposing the ePrivacy Directive.
- 87. Data protection authorities are competent to enforce the GDPR. The mere fact that a subset of the processing falls within the scope of the ePrivacy directive, does not limit the competence of data protection authorities under the GDPR.
- *When exercising their competences, tasks and powers under the GDPR, should data protection authorities take into account the provisions of the ePrivacy Directive, and if so to what extent? In other words, should infringements of national ePrivacy rules be set aside when in assessing compliance with the GDPR, and if so when?*
- 88. The authority or authorities that are appointed as competent in the meaning of the ePrivacy Directive by Member States is exclusively responsible for enforcing the national provisions transposing the ePrivacy Directive that are applicable to that specific processing operation, including in cases where the processing of personal data triggers the material scope of both the GDPR and the ePrivacy Directive. Nevertheless, data protection authorities remain fully competent as regards any processing operations performed upon personal data which are not subject to one or more specific rules contained in the ePrivacy Directive.
- 89. An infringement of the GDPR might also constitute an infringement of national ePrivacy rules. The data protection authority may take this factual finding as to an infringement of ePrivacy rules into consideration when applying the GDPR (e.g., when assessing compliance with the lawfulness or fairness principle under article 5(1)a GDPR). However, any enforcement decision must be justified on the basis of the GDPR, unless the data protection authority has been granted additional competences by Member State law.
- 90. If national law designates the data protection authority as competent authority under the ePrivacy Directive, this data protection authority has the competence to directly enforce national ePrivacy rules in addition to the GDPR (otherwise it does not).

- *To what extent is the cooperation and consistency mechanisms applicable in relation to processing that triggers, at least in relation to certain processing operations, the material scope of both the GDPR and the ePrivacy Directive?*
91. The cooperation and consistency mechanisms available to data protection authorities under Chapter VII of the GDPR, concern the monitoring of the application of GDPR provisions. The GDPR mechanisms do not apply to the enforcement of the national implementation of the ePrivacy Directive. The cooperation and consistency mechanism remains fully applicable, however, insofar as the processing is subject to the general provisions of the GDPR (and not to a “special rule” contained in the ePrivacy Directive).

92. The Board acknowledges that the interpretation above is without prejudice to the outcome of the current negotiations of the ePrivacy Regulation. The proposed Regulation addresses many important elements, including as regards the competences of data protection authorities, but also as regards a range of other very important issues. The Board reiterates its position that the adoption of an ePrivacy Regulation is important.⁴³

For the European Data Protection Board

The Chair

(Andrea Jelinek)

⁴³ The EDPB has called upon the European Commission, Parliament and Council to work together to ensure a swift adoption of the new ePrivacy Regulation (EDPB statement published on 25 May 2018).

Opinion of the Board (Art. 64)



EDPB Plenary meeting, 12-13 March 2019 - Item 2.3.1

Opinion 6/2019 on the draft list of the competent supervisory authority of Spain regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)

Adopted on 12 March 2019

Contents

1	Summary of the Facts.....	4
2	Assessment.....	5
2.1	General reasoning of the EDPB regarding the submitted list	5
2.2	Application of the consistency mechanism to the draft list	5
2.3	Analysis of the draft list	6
	BIOMETRIC DATA	6
	GENETIC DATA.....	6
3	Conclusions / Recommendations.....	6
4	Final Remarks	6

The European Data Protection Board

Having regard to Article 63, Article 64 (1a), (3) - (8) and Article 35 (1), (3), (4), (6) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereafter "GDPR"),

Having regard to Article 51 (1b) of Directive 2016/680 EU on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (hereafter "Law Enforcement Directive").

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018, as revised on 23 November 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (hereafter GDPR) throughout the European Economic Area. In compliance with article 64.1 GDPR, the Board shall issue an opinion where a supervisory authority (SA) intends to adopt a list of processing operations subject to the requirement for a data protection impact assessment pursuant to article 35.4 GDPR. The aim of this opinion is therefore to create a harmonised approach with regard to processing that is cross border or that can affect the free flow of personal data or natural person across the European Union. Even though the GDPR doesn't impose a single list, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by requesting SAs to include some types of processing in their lists, secondly by requesting them to remove some criteria which the Board doesn't consider as necessarily creating high risks for data subjects, and finally by requesting them to use some criteria in a harmonized manner.

(2) With reference to Article 35 (4) and (6) GDPR, the competent supervisory authorities shall establish lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment (hereinafter "DPIA"). They shall, however, apply the consistency mechanism where such lists involve processing operations, which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

(3) While the draft lists of the competent supervisory authorities are subject to the consistency mechanism, this does not mean that the lists should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB assessment/opinion is not to reach a single EU list but rather to avoid significant inconsistencies that may affect the equivalent protection of the data subjects.

(4) The carrying out of a DPIA is only mandatory for the controller pursuant to Article 35 (1) GDPR where processing is “likely to result in a high risk to the rights and freedoms of natural persons”. Article 35 (3) GDPR illustrates what is likely to result in a high risk. This is a non-exhaustive list. The Working Party 29 in the Guidelines on data protection impact assessment¹, as endorsed by the EDPB², has clarified criteria that can help to identify when processing operations are subject to the requirement for a DPIA. The Working Party 29 Guidelines WP248 state that in most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out, however, in some cases a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

(5) The lists produced by the competent supervisory authorities support the same objective to identify processing operations likely to result in a high risk and processing operations, which therefore require a DPIA. As such, the criteria developed in the Working Party 29 Guidelines should be applied when assessing whether the draft lists of the competent supervisory authorities does not affect the consistent application of the GDPR.

(6) Twenty-two competent supervisory authorities received an opinion on their draft lists from the EDPB on 5 September 2018. A further 4 SAs received an opinion on their draft lists on 7 December 2018 and two further SAs received an opinion on the 23 January 2019.

(7) The opinion of the EDPB shall be adopted pursuant to Article 64 (3) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. The competent supervisory authority of Spain has submitted its draft list to the EDPB. The decision on the completeness of the file was taken on 29 January 2019.
2. The period until which the opinion has to be adopted has been set until 8 May 2019.

¹ WP29, Guidelines on Data Protection Impact Assessment and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 (WP 248 rev. 01).

² EDPB, Endorsement 1/2018.

2 ASSESSMENT

2.1 General reasoning of the EDPB regarding the submitted list

3. Any list submitted to the EDPB has been interpreted as further specifying Art 35.1, which will prevail in any case. Thus, no list can be exhaustive.
4. In compliance with article 35.10 GDPR, the Board is of the opinion that if a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of the legal basis the obligation to carry out a DPIA in accordance with paragraphs 1 to 7 of article 35 GDPR does not apply, unless the Member State deems it necessary.
5. Further, if the Board requests a DPIA for a certain category of processing and an equivalent measure is already required by national law, the Agencia Española de Protección de Datos (hereafter Spanish Supervisory Authority) shall add a reference to this measure.
6. This opinion does not reflect upon items submitted by the Spanish Supervisory Authority, which were deemed outside the scope of Article 35.6 GDPR. This refers to items that neither relate “to the offering of goods or services to data subjects” in several Member States nor to the monitoring of the behaviour of data subjects in several Member States. Additionally, they are not likely to “substantially affect the free movement of personal data within the Union”. This is especially the case for items relating to national legislation and in particular where the obligation to carry out a DPIA is stipulated in national legislation. Further, any processing operations that relate to law enforcement were deemed out of scope, as they are not in scope of the GDPR.
7. The Board has noted that several supervisory authorities have included in their lists some types of processing which are necessarily local processing. Given that only cross border processing and processing that may affect the free flow of personal data and data subjects are concerned by Article 35.6, the Board will not comment on those local processing.
8. The opinion aims at defining a consistent core of processing operations that are recurrent in the lists provided by the SAs.
9. This means that, for a limited number of types of processing operations that will be defined in a harmonised way, all the Supervisory Authorities will require a DPIA to be carried out and the Board will recommend the SAs to amend their lists accordingly in order to ensure consistency.
10. When this opinion remains silent on DPIA list entries submitted, it means that the Board is not asking the Spanish Supervisory Authority to take further action.
11. The Spanish Supervisory Authority has notified a translation mistake in the provided list. The term “interested party” thus will be interpreted in the meaning of “Data Subject”, associated with the corresponding rights and freedoms.
12. Finally, the Board recalls that transparency is key for data controllers and data processors. In order to clarify the entries in the list, the Board is of the opinion that making an explicit reference in the lists, for each type of processing, to the criteria set out in the guidelines could improve this transparency.

2.2 Application of the consistency mechanism to the draft list

13. The draft list submitted by the Spanish Supervisory Authority relates to the offering of goods or services to data subjects, relates to the monitoring of their behaviour in several Member States and/or

may substantially affect the free movement of personal data within the Union mainly because the processing operations in the submitted draft list are not limited to data subjects in this country.

2.3 Analysis of the draft list

14. Taking into account that:
 - a. Article 35 (1) GDPR requires a DPIA when the processing activity is likely to result in a high risk to the rights and freedoms of natural persons; and
 - b. Article 35 (3) GDPR provides a non-exhaustive list of types of processing that require a DPIA, the Board is of the opinion that:

BIOMETRIC DATA

15. The list submitted by the Spanish Supervisory Authority for an opinion of the Board does not currently require a DPIA to be done for the processing of biometric data for the purpose of uniquely identifying a natural person. As such, the Board requests the Spanish Supervisory Authority to amend its list accordingly, by adding explicitly the processing of biometric data for the purpose of uniquely identifying a natural person in conjunction with at least one other criterion to its list, to be applied without prejudice to article 35(3) GDPR.

GENETIC DATA

16. The list submitted by the Spanish Supervisory Authority for an opinion of the Board does not currently require a DPIA to be done for the processing of genetic data. . The Board is of the opinion that the processing of genetic data on its own is not necessarily likely to represent a high risk. However, the processing of genetic data in conjunction with at least one other criterion requires a DPIA to be carried out. As such, the Board requests the Spanish Supervisory Authority to amend its list accordingly, by adding explicitly the processing of genetic data in conjunction with at least one other criterion to its list, to be applied without prejudice to article 35(3) GDPR.

3 CONCLUSIONS / RECOMMENDATIONS

17. The draft list of the Spanish Supervisory Authority may lead to an inconsistent application of the requirement for a DPIA and the following changes need to be made:
 - Regarding biometric data: the Board requests the Spanish Supervisory Authority to amend its list accordingly, by adding explicitly the processing of biometric data for the purpose of uniquely identifying a natural person in conjunction with at least one other criterion to its list.
 - Regarding genetic data: the Board requests the Spanish Supervisory Authority to amend its list by adding explicitly the processing of genetic data in conjunction with at least one other criterion to its list.

4 FINAL REMARKS

18. This opinion is addressed to the Spanish Supervisory Authority and will be made public pursuant to Article 64 (5b) GDPR.
19. According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. The supervisory authority shall communicate the final decision to the Board for inclusion in

the register of decisions which have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

EDPB oral pleading before the Court of Justice of the EU

Case C-311/18 (Facebook Ireland and Schrems)

9th July 2019, 9h00

Luxembourg

With regard to the first question on standard contractual clauses (SCCs):

- The SCCs adopted by the COM are instruments with a general scope. They are not related to any specific third country. They are provided for an individual transfer contract from an EU-exporter to a third country importer.
- Therefore, the EDPB considers that the COM is not obliged to examine whether the access of the public authorities of a given third country to the data transferred respects the level of protection required by EU law.
- The EDPB considers that this is primarily the responsibility of the exporter and the importer, when considering whether to enter into the SCCs.
- This means that it is also for SAs, in particular on the basis of a complaint, to assess whether the continuity of the protection afforded by Union law is ensured once the data were transferred, including whether the

exporter and importer complied with their obligations under the SCCs. If not, SAs may suspend transfers.

- Under SCCs, SAs are only empowered to assess individual cases but do not have the power to issue a general ban of transfers to a specific third country.

As far as the second question is concerned, on data during the stage of transit:

- On the first part of the question: The EDPB takes the view that the continuity of the protection afforded under EU laws needs to be ensured, also during the stage of transit to a third country, no matter which transfer tool is used.
- In the context of an assessment of adequacy, when assessing the level of protection of the laws of a third country the EDPB has stated that COM's analysis should not be limited to the law and practice allowing for surveillance within that country's physical borders. It should also cover the law and practice allowing for surveillance outside or on its way to its physical borders, as far as EU data are concerned.
- The EDPB takes the view that, no matter which Chapter V GDPR transfer tool is used, the assessment should be limited to applicable laws and practices in the third country where the recipient is. The EDPB sees no obligation to assess any other country's laws which could provide for the possibility to intercept data on their way to the third country where the recipient is.

- With regard to the U.S., the EDPB included the Executive Order 12333, which applies to the collection of data by the U.S. authorities outside the U.S. territory, and the Presidential Policy Directive 28 (PPD-28), when commenting on the Privacy Shield decision and its joint reviews.
- On the second part of the question: the adoption of an adequacy decision may create a presumption, if the respect for the level of protection during the stage of transit was made part of the adequacy finding.
- Though the EDPB notes that reference is made to data in transit in the Privacy Shield adequacy decision, the level of protection during the stage of transit was not discussed during both Privacy Shield Joint Reviews, as the U.S. Government stated that the stage of transit is not covered by the Privacy Shield.

In relation to the third question on the level of protection required:

- The EDPB takes the view that, in order to assess the legal framework of a third country, all domestic rules should be taken into account when making an assessment of adequacy. This includes the limits within which the administration of that third country may collect data, as long as those domestic rules are publicly available, sufficiently clear and precise, and binding on the administration.
- At the same time, the EDPB would like to stress that the level of protection in the third country can only be ensured by laws of the third country which confer enforceable and effective rights on the data subject and which can be relied on before courts or tribunals.

With reference to the fourth question, on access to personal data by a public authority:

- In our view, as the screening of communications and access to data in this context are inextricably linked to the process of collection of data, the access to data by means of selectors for the purposes of screening communications is part of the processing of the data collected.
- I would like to refer to the specific context of the Privacy Shield, in particular with regard to US programmes run under the authority of 702 FISA, which aim at collecting personal data by means of selectors following the screening of communications. The EDPB, in its reports on the 1st and 2nd Joint Reviews of the Privacy Shield, stressed the importance of more specific safeguards for these measures, for example for precise targeting to determine whether an individual or a group can be a target of surveillance, and for strict scrutiny of individual targets by an independent authority ex-ante.

Regarding the fifth question, on the Privacy Shield Ombudsperson:

- The EDPB welcomed the establishment of the Ombudsperson mechanism as a new redress mechanism.
- At the same time, the EDPB expressed concern with regard to effective judicial redress before the courts of the U.S., and examined if the Ombudsperson mechanism could have offset these deficiencies with respect to individual judicial protection. The EDPB took the view that the

Ombudsperson mechanism could only offset the deficiencies of judicial redress if the requirements of Art. 47 of the Charter are met.

- The EDPB thus focused on the question how independent the Ombudsperson is and what powers she/he has.
- The EDPB stated in the last Privacy Shield joint review issued earlier this year that it is not in a position to conclude that the Ombudsperson is vested with sufficient powers to access information and to remedy non-compliance. The EDPB went on to say it can thus not state that the Ombudsperson can be considered an “effective remedy before a tribunal” in the meaning of Art. 47 of the Charter of Fundamental Rights.

In relation to the sixth question, on the US Government’s replies:

- The EDPB refrains from commenting on the replies by the United States Government.

Finally, I would like to make some additional remarks:

- Personal data of Europeans are well protected through the high European standards provided and enshrined in the Charter of Fundamental Rights and the GDPR.
- As one of the judges of this court said after the Schrems I ruling, this protection “is sailing with the data, wherever the data are transferred to”.
- We, the SAs, used our powers and capacities to uphold this standard and to spread it, bearing in mind consideration 42 of the Schrems I ruling

stating “*that national SA must in particular ensure a fair balance between, on the one hand, observance of the fundamental right to privacy and on the other hand, the interests requiring free movement of personal data*”, and recital 4 of the GDPR.

Andrea Jelinek

Chair of the European Data Protection Board

Opinion of the Board (Art. 64)



EDPB Plenary meeting, 12-13 March 2019 - Item 2.3.1

Opinion 7/2019 on the draft list of the competent supervisory authority of Iceland regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)

Adopted on 12 March 2019

Contents

1	Summary of the Facts.....	4
2	Assessment.....	5
2.1	General reasoning of the EDPB regarding the submitted list	5
2.2	Application of the consistency mechanism to the draft list	5
2.3	Analysis of the draft list	6
	SCOPE OF THE DRAFT DECISION	6
	EMPLOYEE MONITORING	6
3	Conclusions / Recommendations.....	6
4	Final Remarks	6

Adopted

The European Data Protection Board

Having regard to Article 63, Article 64 (1a), (3) - (8) and Article 35 (1), (3), (4), (6) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereafter "GDPR"),

Having regard to Article 51 (1b) of Directive 2016/680 EU on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (hereafter "Law Enforcement Directive").

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018, as revised on 23 November 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (hereafter GDPR) throughout the European Economic Area. In compliance with article 64.1 GDPR, the Board shall issue an opinion where a supervisory authority (SA) intends to adopt a list of processing operations subject to the requirement for a data protection impact assessment pursuant to article 35.4 GDPR. The aim of this opinion is therefore to create a harmonised approach with regard to processing that is cross border or that can affect the free flow of personal data or natural person across the European Union. Even though the GDPR doesn't impose a single list, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by requesting SAs to include some types of processing in their lists, secondly by requesting them to remove some criteria which the Board doesn't consider as necessarily creating high risks for data subjects, and finally by requesting them to use some criteria in a harmonized manner.

(2) With reference to Article 35 (4) and (6) GDPR, the competent supervisory authorities shall establish lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment (hereinafter "DPIA"). They shall, however, apply the consistency mechanism where such lists involve processing operations, which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

(3) While the draft lists of the competent supervisory authorities are subject to the consistency mechanism, this does not mean that the lists should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB assessment/opinion is not to reach a single EU list but rather to avoid significant inconsistencies that may affect the equivalent protection of the data subjects.

(4) The carrying out of a DPIA is only mandatory for the controller pursuant to Article 35 (1) GDPR where processing is “likely to result in a high risk to the rights and freedoms of natural persons”. Article 35 (3) GDPR illustrates what is likely to result in a high risk. This is a non-exhaustive list. The Working Party 29 in the Guidelines on data protection impact assessment¹, as endorsed by the EDPB², has clarified criteria that can help to identify when processing operations are subject to the requirement for a DPIA. The Working Party 29 Guidelines WP248 state that in most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out, however, in some cases a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

(5) The lists produced by the competent supervisory authorities support the same objective to identify processing operations likely to result in a high risk and processing operations, which therefore require a DPIA. As such, the criteria developed in the Working Party 29 Guidelines should be applied when assessing whether the draft lists of the competent supervisory authorities does not affect the consistent application of the GDPR.

(6) Twenty-two competent supervisory authorities received an opinion on their draft lists from the EDPB on 5 September 2018. A further four SAs received an opinion on their draft lists on 4 December 2018 and two further received an opinion on their list on 23 January 2019.

(7) The opinion of the EDPB shall be adopted pursuant to Article 64 (3) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. The competent supervisory authority of Iceland has submitted its draft list to the EDPB. The decision on the completeness of the file was taken on 4 February 2019.
2. The period until which the opinion has to be adopted has been set until 2 April 2019.

¹ WP29, Guidelines on Data Protection Impact Assessment and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 (WP 248 rev. 01).

² EDPB, Endorsement 1/2018.

2 ASSESSMENT

2.1 General reasoning of the EDPB regarding the submitted list

3. Any list submitted to the EDPB has been interpreted as further specifying Art 35.1, which will prevail in any case. Thus, no list can be exhaustive.
4. In compliance with article 35.10 GDPR, the Board is of the opinion that if a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of the legal basis the obligation to carry out a DPIA in accordance with paragraphs 1 to 7 of article 35 GDPR does not apply, unless the Member State deems it necessary.
5. Further, if the Board requests a DPIA for a certain category of processing and an equivalent measure is already required by national law, the Persónuvernd (hereafter Icelandic Supervisory Authority) shall add a reference to this measure.
6. This opinion does not reflect upon items submitted by the Icelandic Supervisory Authority, which were deemed outside the scope of Article 35.6 GDPR. This refers to items that neither relate “to the offering of goods or services to data subjects” in several Member States nor to the monitoring of the behaviour of data subjects in several Member States. Additionally, they are not likely to “substantially affect the free movement of personal data within the Union”. This is especially the case for items relating to national legislation and in particular where the obligation to carry out a DPIA is stipulated in national legislation. Further, any processing operations that relate to law enforcement were deemed out of scope, as they are not in scope of the GDPR.
7. The Board has noted that several supervisory authorities have included in their lists some types of processing which are necessarily local processing. Given that only cross border processing and processing that may affect the free flow of personal data and data subjects are concerned by Article 35.6, the Board will not comment on those local processing.
8. The opinion aims at defining a consistent core of processing operations that are recurrent in the lists provided by the SAs.
9. This means that, for a limited number of types of processing operations that will be defined in a harmonised way, all the Supervisory Authorities will require a DPIA to be carried out and the Board will recommend the SAs to amend their lists accordingly in order to ensure consistency.
10. When this opinion remains silent on DPIA list entries submitted, it means that the Board is not asking the Icelandic Supervisory Authority to take further action.
11. Finally, the Board recalls that transparency is key for data controllers and data processors. In order to clarify the entries in the list, the Board is of the opinion that making an explicit reference in the lists, for each type of processing, to the criteria set out in the guidelines could improve this transparency.

2.2 Application of the consistency mechanism to the draft list

12. The draft list submitted by the Icelandic Supervisory Authority relates to the offering of goods or services to data subjects, relates to the monitoring of their behaviour in several Member States and/or may substantially affect the free movement of personal data within the Union mainly because the processing operations in the submitted draft list are not limited to data subjects in this country.

2.3 Analysis of the draft list

13. Taking into account that:
 - a. Article 35 (1) GDPR requires a DPIA when the processing activity is likely to result in a high risk to the rights and freedoms of natural persons; and
 - b. Article 35 (3) GDPR provides a non-exhaustive list of types of processing that require a DPIA, the Board is of the opinion that:

SCOPE OF THE DRAFT DECISION

14. The Icelandic SA states in some cases that its list includes processing activities that the Icelandic DPA considers to be of high risk to the rights and freedoms of data subjects. However, the Board recalls that the GDPR states that the list that have to be published by the supervisory authorities are the lists of processing that are likely to result in a high risk for the rights and freedoms of data subjects. The Board therefore requests the Icelandic Authority to amend its list by aligning its wording with the wording of Article 35.1 of the GDPR.

EMPLOYEE MONITORING

15. The Board takes note of the inclusion of “processing of personal data involving measures for systematic monitoring of employee activities” in the Icelandic DPIA list. The Board recalls that in its view WP249 of the Article 29 working party remain valid when defining the concept of systematic processing of employee data.

3 CONCLUSIONS / RECOMMENDATIONS

16. The draft list of the Icelandic Supervisory Authority may lead to an inconsistent application of the requirement for a DPIA and the following changes need to made:
 - Regarding the scope of the list: the Board requests the Icelandic Supervisory Authority to amend its list by stating that the types of processing listed are the one that are likely to present high risks for the rights and freedom of data subjects.

4 FINAL REMARKS

17. This opinion is addressed to the Icelandic Supervisory Authority and will be made public pursuant to Article 64 (5b) GDPR.
18. According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. The supervisory authority shall communicate the final decision to the Board for inclusion in the register of decisions which have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Adopted

Work program



CSC meeting, 08 July 2020

Work program 2020-2022

Contents

1. INTRODUCTION	2
2. WORKING METHODS	3
2.1 Distribution of roles	3
2.2 Organisation of the meetings	3
2.3 Technical tools	4
2.4 Communication and visual identity	4
2.5 Dialogue and engagement with controllers, processors and third parties	4
3. PLANNED ACTIVITIES.....	5
3.1 Promote and facilitate the exercise of data subject's rights	5
3.2 Examine difficulties of interpretation or application of EU and national law	6
3.3 Exchange information and conduct joint audits or coordinated inspections.....	7
3.4 Prepare for the start of the EPPO's activities and other EU bodies and information systems that will fall under the Committee's scope	8

1. INTRODUCTION

Over the last years, EU large-scale information systems connecting EU Member States' authorities and EU bodies have increased and evolved. These systems enable them to share electronically personal data in an unprecedented speed and volume.

Whereas the European Data Protection Supervisor (EDPS) supervises the EU bodies' processing of data, national supervisory authorities supervise national authorities, from which most data originates and to which data is ultimately channelled. It thus becomes essential that they coordinate their supervisory activities

Regulation 2018/1725 makes this cooperation between the EDPS and the national supervisory authorities an obligation¹. This Regulation specifies some forms this cooperation could take, such as exchanging information; assisting each other in carrying out audits and inspections; examining difficulties of interpretation or application of this Regulation and other applicable EU laws; studying problems with the exercise of independent supervision or of data subject rights; preparing harmonised proposals for solutions to problems identified; and promoting awareness of data protection rights.

To ensure and facilitate this cooperation, Regulation 2018/1725 provides that the EDPS and national supervisory authorities meet at least twice a year within the framework of the European Data Protection Board. This led to the recent creation of the Coordinated Supervision Committee (CSC).

The Committee can only exercise its activities with respect to those EU large-scale information systems and bodies whose legal acts refer to Article 62 of Regulation 2018/1725 or to the European Data Protection Board, and by implication, to the CSC.

On this basis and due to the recent character of Regulation 2018/1725 the Committee's scope currently covers the Internal Market Information system (IMI)², Eurojust,³ and the upcoming European Public Prosecutor Office (EPPO)⁴, which is expected for December 2020.

Other mechanisms preceding the Committee ensure the coordinated supervision of other EU large-scale information systems and bodies that predate Regulation 2018/1725. The Committee will progressively cover these large-scale information systems and EU bodies in the coming years, insofar as their legal basis are revised. The Committee will also cover the new information systems and EU bodies to be created, such as the European Entry/Exit System (EES) and the European Travel Information and Authorisation System (ETIAS).

The 1st meeting of the Committee was held on 3 December 2019. During its first meeting, the Committee elected Giuseppe Busia from the Italian supervisory authority as Coordinator and Iris Gnedler from the German Federal supervisory authority as Deputy Coordinator for a term of two years. The Committee also adopted its Rules of Procedure.

¹ Article 62 of the Regulation (EU) 2018/1725

² Article 21.3 of the IMI Regulation (EU) 2018/1724

³ Article 42.2 of the Eurojust Regulation (EU) 2018/1727

⁴ Article 87 of the EPPO Regulation (EU) 2017/1939

2. WORKING METHODS

2.1 Distribution of roles

The Committee elects a Coordinator and at least a Deputy Coordinator from among its members for a term of office of two years.⁵

The Coordinator convenes and chairs the meetings, acts as a contact point in CSC matters, sets the draft agenda, carries out all the tasks that have been assigned to him/her in the Rules of Procedure and updates the European Data Protection Board of the work of the Committee at least twice a year. The Deputy Coordinator will perform these tasks if the Coordinator is unable to attend. Both cooperate in liaison with the Secretariat to ensure the smooth functioning of the Committee, prepare the draft agenda, the draft work program and the draft joint report of activities on coordinated supervision the Committee will adopt.⁶

The EDPB Secretariat will also provide the Secretariat of the Committee.⁷ The Secretariat assists the Committee in the performance of its tasks and acts solely in the best interests of the Committee.

The Committee or the Coordinator may designate one or several (co-) rapporteur(s) for specific issues. They will be responsible for the elaboration of documents, incorporating comments into revised drafts, finalizing the document and presenting them to the Committee.⁸

2.2 Organisation of the meetings

The Committee must meet at least twice a year.⁹ The Coordinator may also decide to convene extraordinary meetings, on its own initiative or at the request of the majority of the Committee's participating authorities.¹⁰ The Secretariat shares the invitations, the draft agenda and the meeting documents with each member of the Committee at least 10 days in advance of the meeting.¹¹ In exceptional circumstances, documents may be distributed later.

Meetings of the Committee can only take place if at least half of the participating authorities or their representatives are attending.¹² The Committee will approve the agenda at the beginning of each meeting.¹³

The costs and the servicing of the Committee's meetings are borne by the EDPB Secretariat.

⁵ Article 3 of the Rules of Procedure

⁶ Article 4 of the Rules of Procedure

⁷ Article 17 of the Rules of Procedure

⁸ Article 8 of the Rules of Procedure

⁹ Article 12.1 of the Rules of Procedure

¹⁰ Article 12.3 of the Rules of Procedure

¹¹ Article 14 of the Rules of Procedure

¹² Article 12.5 of the Rules of Procedure

¹³ Article 13.4 of the Rules of Procedure

The COVID-19 crisis has led EU institutions to adapt to new ways of working and to hold meetings remotely to be able to continue their activity. The Committee has also resorted to remote meetings to hold its meeting of 8 July 2020 and may need to do so again in the future.

In ordinary times, remote meetings can also be a useful way to lighten the agenda of the Committee in-person meetings, improve the Committee's efficiency and the quality of its work. The Committee could organize remote meetings to address matters that could be discussed briefly and/or that could not wait for the in-person meetings. The Committee could leave to in-person meetings matters that may be more complex and require longer discussions.

2.3 Technical tools

The Committee has a functional mailbox within the EDPB mailbox for all correspondences of the Committee. The Secretariat is in charge of handling this functional mailbox, answering questions and requests of members and redirecting emails from third parties to the Coordinator or participating authorities where needed. The Secretariat also uses the functional mailbox to issue the invitations, the draft agenda and the documents for the meetings.

The Secretariat also uses the Confluence system as its main tool for sharing information with the participants. The Committee has a dedicated section with a forum, subsections for each of the CSC meetings, a section for the work items overview, and resources made available and/or produced by the CSC members, such as legal references, interpretative guidelines, best practices and others.

2.4 Communication and visual identity

The Committee will have a dedicated website where all public documents of the Committee will be available.

The Committee also has its own logo, which it uses in all of its documents and its website.

2.5 Dialogue and engagement with controllers, processors and third parties

The Committee should seek, through its activities and meetings, a regular dialogue and engagement with controllers, processors and third parties, including civil society organisations to ensure a comprehensive reflexion on the issues at stake, while always taking into account its role as independent body.

3. PLANNED ACTIVITIES

The Committee has foreseen the following activities in the work program to:

- Ensure that data subjects are able to exercise their rights;
- Reach a common understanding between its participating authorities on their respective scope of supervision, applicable legal basis, and the areas where they need to cooperate and coordinate, from the beginning of the Committee's activities;
- Prepare the Committee's work on the supervision of the European Public Prosecutor's Office and other large-scale information systems that will fall within the Committee's remit in the coming years.

The Committee will be flexible and also work on other activities that may not be included in this work program and that participating authorities may bring to its attention, based on their relevance, urgency or unforeseen character.

3.1 Promote and facilitate the exercise of data subject's rights

One of the main legal tasks of the Committee is to study problems with the exercise of independent supervision or with the exercise of the rights of data subjects and propose solutions to these problems.¹⁴.

Large-scale EU information systems and networks such as IMI, Eurojust, and EPPO, which connect in a seamless manner EU and national authorities, have a hybrid nature: both national-EU and trans-European. Data may transit and be stored in multiple places and be processed by diverse entities. A data subject may not know at a given point in time if his/her data is being processed at EU and/or at national level and thus to whom address his/her requests.

In this complexity, supervisory authorities must cooperate and coordinate their actions to enable data subjects to exercise their rights effectively. The EDPS and national supervisory authorities must maintain close contact to determine their competence over such requests and refer them to each other where relevant. They must also ensure that any decision they may take further to a data subject's request, such as to rectify or erase his/her personal data, duly takes into consideration any national objection or exception EU and national laws may foresee, for example to preserve the integrity of criminal proceedings.

¹⁴ Article 62.2 of the (EU) Regulation 2018/1725

The Committee will conduct the following tasks under this activity:

- **Revise the information available to data subjects on how they may exercise their rights:** the Committee will take stock of the information currently available to data subjects on the information systems and EU bodies' falling under the Committee's purview. It will also propose changes if necessary to ensure that this information is up to date with the latest developments of EU data protection law and presented in a concise, intelligible and easily accessible form using clear and plain language.
- **Produce a list of national competent authorities for data subjects' request:** the Committee will draw an updated list of national authorities competent to receive requests from data subjects on the systems and EU bodies' falling within its remit with their contact details and make it available to the public.
- **Exchange best practices on data subject's rights and produce guides for the benefit of all supervisory authorities:** national supervisory authorities will have diverse experiences in protecting and enforcing data subject's rights in relation to EU large-scale information systems and bodies. They will put in common their practices and compile those having demonstrated their value and efficiency in a guide.
- **Produce a report with proposals on the exercise of data subject's rights:** The Committee will produce at the end of the programmed period a report with proposals on the exercise of data subject's rights. This report will give the Committee an active role in the creation of a mechanism that streamlines the exercise of data subject rights, and provides data subjects with adequate information and assistance to this end.

3.2 Examine difficulties of interpretation or application of EU and national law

Another legal task of the Committee is to examine difficulties of interpretation or application of Regulation 2018/1725 and other EU laws to their activities in relation to EU large-scale information systems and bodies.

To be able to apply effectively and in harmonized manner EU law to their activities, supervisory authorities need to reach a common understanding on the interplay between EU instruments with a general nature (such as Regulations 2018/1725 and Directive 2016/680) and a specialized nature (such as the IMI,¹⁵ Eurojust¹⁶ and EPPO¹⁷ Regulations).

The application of some of these EU instruments also needs to be reconciled with the application of national law, which may apply for instance to the processing of law enforcement data.

¹⁵ Regulation (EU) 2018/1724

¹⁶ Regulation (EU) 2018/1727

¹⁷ Regulation (EU) 2017/1939

This can be a complex endeavour and bring to the fore differences in the legislation, interpretation of EU law, and practice across EU Member States. Some recent EU instruments, such as the EPPO Regulation, underline the role of the Committee in addressing these difficulties.¹⁸

The Committee will carry out the following tasks under this activity:

- **Conduct a study and produce a report on the interplay between EU and national law and its application to the activities of supervisors:** the Committee will build on recent studies the EDPB is conducting, such as its ongoing study on the national implementation of Article 45 of the LED; input from the Committee members expressed through surveys and questionnaires; and academic research. The Committee's work will result in a report containing concrete proposals that would be ready by the end of the programming period.
- **Monitor the implementation of the framework for the interoperability of EU information systems:** the new rules establishing a framework for interoperability between EU information systems in the field of borders and visa (Regulation (EU) 2019/817) and in the field of police and judicial cooperation, asylum and migration (Regulation (EU) 2019/818), are now progressively being implemented including through implementing acts to be adopted by the European Commission. As several of the concerned information systems will fall under the scope of the supervision activities of the Committee, attention will be paid to the implementation of this overall framework, both from a legal and operational point of view, with a view to ensuring consistency and coherence with the EU *acquis* in the field of data protection.

3.3 Exchange information and conduct joint audits or coordinated inspections

One of the Committee's *raison d'être* is to enable supervisory authorities to exchange relevant information and assist each other in carrying out audits and inspections.¹⁹ Information exchange and mutual assistance are necessary because of the complexity and size of the information systems supervised, the transiting and retention of personal data across various national and EU information systems, and the multiple and diverse data controllers, processors, data subjects and other parties that may be involved.

Supervisory authorities are already experienced in supervising EU bodies and large-scale information systems such as Europol, SIS, CIS, Eurodac and others. Building on this experience, they will be able to identify those processing operations or practices involving personal data in relation to IMI, Eurojust and soon, the EPPO, that require or could benefit from an exchange of information and assistance at European level.

¹⁸ Article 87 of the EPPO (EU) Regulation 2017/1939

¹⁹Article 62.2 of the (EU) Regulation 2018/1725

The Committee will conduct the following tasks under this activity:

- **Develop general standards or reference frameworks for national audits and inspections:** the Committee will work on identifying key elements and principles to be taken into account by supervisory authorities when carrying out audit and inspections, possibly integrated into general standards or reference frameworks for each information system with a view to ensuring consistency of supervision activities and reporting;
- **Collect information and promote best practices:** the Committee members will be able to draw from their experience supervising EU large-scale information systems and bodies, such as SIS, Eurojust and Europol, information and best practices. For example, the Committee will collect information on the legacy of the Eurojust Joint Supervisory Body (JSB), in particular the activities and reports in relation to the national competent authorities, by coordinating with the EDPS, which took over the supervision at central level. Information and best practices will be collected in a guide or report.

Supervisory authorities and public authorities acting as controllers, such as the European Commission, Eurojust and the EPPO, share their mandate to serve EU citizens. There are potential and still unexplored venues for an effective dialogue between these public authorities that could be beneficial for them and in turn, for EU citizens. Such dialogue should also involve civil society organisation to ensure a comprehensive reflexion on the issues at stake.

The Committee should, through its activities and meetings, ensure a regular engagement with controllers, processors and third parties, including civil society organisations.

3.4 Prepare for the start of the EPPO's activities and other EU bodies and information systems that will fall under the Committee's scope

The European Public Prosecutor's Office (EPPO) is expected to start its operations on December 2020. The EPPO will process in its electronic case management system special categories of personal data and data relating to criminal convictions and offences for its conduct of criminal investigations and prosecutions.

The EPPO's first steps deserve the Committee's attention to help the EPPO and those EU Member States' authorities participating in it ensure that they apply correctly, from the outset, data protection principles such as purpose limitation, data minimisation, limited storage periods, data quality, data security, data protection by design and by default, and relevant data protection safeguards.

Other existing or upcoming systems that will raise similar data protection issues and over which the Committee will become competent during the period (2020-2022) will be:

- The Entry/Exit System (EES): expected for 2021;
- The Schengen Information System (SIS): no later than 28 December 2021;
- The European Travel Information and Authorisation System (ETIAS): expected for 2022;
- The European Criminal Records Information System (ECRIS-TCN): expected for 2022.

The Committee will carry out the following tasks under this activity:

- **Identify based on the current legal framework those areas of the EPPO that could present high risks to individual rights:** although the EPPO has not yet begun its operations, the Committee members will proactively identify those future processing operations or areas that will require their attention and anticipate issues. They will do so based on the EPPO's legal basis and planned set-up, and their experience supervising EU bodies working in similar areas, such as Europol and Eurojust. The Committee will then produce a report with findings and recommendations for the benefit of supervisory authorities and controllers.
- **Prepare the Committee's assumption of the coordinated supervision over SIS:** the Schengen Information System is one of the most complex and widely used large-scale EU information system. It is also one of the biggest databases in the world for the purpose of border control of people and objects. The Schengen Information System II Supervision Coordination Group ("SIS II SCG") has so far ensured its coordinated supervision, although it will pass the baton to the Committee by December 2021, as envisaged. To be fully prepared for this moment, the Committee will dedicate special items in its meetings and channels of information to this transition, and ensure the transfer of knowledge and experience between the SIS II SCG and the Committee.
- **Follow the preparation of the new large-scale EU Information Systems:** the Committee must prepare for the entry into operation of the EES, ETIAS, and ECRIS-TCN, in 2021 and 2022. These systems are of a technical and complex nature and raise especially sensitive data protection issues owing to the foreseen interoperability between them. The Committee will also foresee dedicated items in its meetings to these systems and invite representatives from the controllers and other technical experts to discuss its future operations and identify high risks in relation to data protection.

Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*

Adopted on 23 July 2020

This document aims at presenting answers to some frequently asked questions received by supervisory authorities ("SAs") and will be developed and complemented along with further analysis, as the EDPB continues to examine and assess the judgment of the Court of Justice of the European Union (the "Court").

The judgment C-311/18 can be found [here](#), and the press release of the Court may be found [here](#).

1) What did the Court rule in its judgment?

- ➔ In its judgment, the Court examined the validity of the European Commission's Decision 2010/87/EC on Standard Contractual Clauses ("SCCs") and considered it is valid. Indeed, the validity of that decision is not called into question by the mere fact that the standard data protection clauses in that decision do not, given that they are contractual in nature, bind the authorities of the third country to which data may be transferred.

However, that validity, the Court added, depends on whether the 2010/87/EC Decision includes effective mechanisms that make it possible, in practice, to ensure compliance with the level of protection essentially equivalent to that guaranteed within the EU by the GDPR and that transfers of personal data pursuant to such clauses are suspended or prohibited in the event of the breach of such clauses or it being impossible to honour them.

In that regard, the Court points out, in particular, that the 2010/87/EC Decision imposes an obligation on a data exporter and the recipient of the data (the "data importer") to verify, prior to any transfer, and taking into account the circumstances of the transfer, whether that level of protection is respected in the third country concerned, and that the 2010/87/EC Decision requires the data importer to inform the data exporter of any inability to comply with the standard data protection clauses, and where necessary with any supplementary measures to those offered by those clause, the data exporter then being, in turn, obliged to suspend the transfer of data and/or to terminate the contract with the data importer

- ➔ The Court also examined the validity of the Privacy Shield Decision (Decision 2016/1250 on the adequacy of the protection provided by the EU-U.S. Privacy Shield), as the transfers at stake in the context of the national dispute leading to the request for preliminary ruling took place between the EU and the United States (“U.S.”).

The Court considered that the requirements of U.S. domestic law, and in particular certain programmes enabling access by U.S. public authorities to personal data transferred from the EU to the U.S. for national security purposes, result in limitations on the protection of personal data which are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required under EU law¹, and that this legislation does not grant data subjects actionable rights before the courts against the U.S. authorities.

As a consequence of such a degree of interference with the fundamental rights of persons whose data are transferred to that third country, the Court declared the Privacy Shield adequacy Decision invalid.

2) Does the Court’s judgment have implications on transfer tools other than the Privacy Shield?

- ➔ In general, for third countries, the threshold set by the Court also applies to all appropriate safeguards under Article 46 GDPR used to transfer data from the EEA to any third country. U.S. law referred to by the Court (i.e., Section 702 FISA and EO 12333) applies to any transfer to the U.S. via electronic means that falls under the scope of this legislation, regardless of the transfer tool used for the transfer².

3) Is there any grace period during which I can keep on transferring data to the U.S. without assessing my legal basis for the transfer?

- ➔ No, the Court has invalidated the Privacy Shield Decision without maintaining its effects, because the U.S. law assessed by the Court does not provide an essentially equivalent level of protection to the EU. This assessment has to be taken into account for any transfer to the U.S.

4) I was transferring data to a U.S. data importer adherent to the Privacy Shield, what should I do now?

- ➔ Transfers on the basis of this legal framework are illegal. Should you wish to keep on transferring data to the U.S., you would need to check whether you can do so under the conditions laid down below.

5) I am using SCCs with a data importer in the U.S., what should I do?

- ➔ The Court found that U.S. law (i.e., Section 702 FISA and EO 12333) does not ensure an essentially equivalent level of protection.

¹ The Court underlines that certain surveillance programmes enabling access by U.S. public authorities to personal data transferred from the EU to the U.S. for national security purposes do not provide for any limitations on the power conferred on the U.S. authorities, or the existence of guarantees for potentially targeted non-US persons.

² Section 702 FISA applies to all “electronic communication service provider” (see the definition under 50 USC § 1881(b)(4)), while EO 12 333 organises electronic surveillance, which is defined as the “acquisition of a non-public communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a non electronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter” (3.4; b)).

Whether or not you can transfer personal data on the basis of SCCs will depend on the result of your assessment, taking into account the circumstances of the transfers, and supplementary measures you could put in place. The supplementary measures along with SCCs, following a case-by-case analysis of the circumstances surrounding the transfer, would have to ensure that U.S. law does not impinge on the adequate level of protection they guarantee.

If you come to the conclusion that, taking into account the circumstances of the transfer and possible supplementary measures, appropriate safeguards would not be ensured, you are required to suspend or end the transfer of personal data. However, if you are intending to keep transferring data despite this conclusion, you must notify your competent SA³.

6) I am using Binding Corporate Rules (“BCRs”) with an entity in the U.S., what should I do?

- ➔ Given the judgment of the Court, which invalidated the Privacy Shield because of the degree of interference created by the law of the U.S. with the fundamental rights of persons whose data are transferred to that third country, and the fact that the Privacy Shield was also designed to bring guarantees to data transferred with other tools such as BCRs, the Court’s assessment applies as well in the context of BCRs, since U.S. law will also have primacy over this tool.

Whether or not you can transfer personal data on the basis of BCRs will depend on the result of your assessment, taking into account the circumstances of the transfers, and supplementary measures you could put in place. These supplementary measures along with BCRs, following a case-by-case analysis of the circumstances surrounding the transfer, would have to ensure that U.S. law does not impinge on the adequate level of protection they guarantee.

If you come to the conclusion that, taking into account the circumstances of the transfer and possible supplementary measures, appropriate safeguards would not be ensured, you are required to suspend or end the transfer of personal data. However if you are intending to keep transferring data despite this conclusion, you must notify your competent SA⁴.

7) What about other transfer tools under Article 46 GDPR?

- ➔ The EDPB will assess the consequences of the judgment on transfer tools other than SCCs and BCRs. The judgement clarifies that the standard for appropriate safeguards in Article 46 GDPR is that of “essential equivalence”.

As underlined by the Court, it should be noted that Article 46 appears in Chapter V GDPR, and, accordingly, must be read in the light of Article 44 GDPR, which lays down that *“all provisions in that chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by that regulation is not undermined”*.

³ See in particular recital 145 of the Court’s judgment, and Clause 4(g) Commission decision 2010/87/EU, as well as Clause 5(a) Commission Decision 2001/497/EC and Annex Set II (c) of Commission Decision 2004/915/EC.

⁴ See in particular recital 145 of the Court’s judgment and Clause 4(g) of Commission Decision 2010/87/EU. See also Section 6.3 WP256 rev.01 (Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in BCRs, endorsed by the EDPB, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109), and Section 6.3 WP257 rev.01 (Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Processor BCRs, endorsed by the EDPB, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110).

8) Can I rely on one of the derogations of Article 49 GDPR to transfer data to the U.S.?

- It is still possible to transfer data from the EEA to the U.S. on the basis of derogations foreseen in Article 49 GDPR provided the conditions set forth in this Article apply. The EDPB refers to its guidelines on this provision⁵.

In particular, it should be recalled that when transfers are based on the consent of the data subject, it should be:

- explicit,
- specific for the particular data transfer or set of transfers (meaning that the data exporter must make sure to obtain specific consent before the transfer is put in place even if this occurs after the collection of the data has been made), and
- informed, particularly as to the possible risks of the transfer (meaning the data subject should also be informed of the specific risks resulting from the fact that their data will be transferred to a country that does not provide adequate protection and that no adequate safeguards aimed at providing protection for the data are being implemented).

With regard to transfers necessary for the performance of a contract between the data subject and the controller, it should be borne in mind that personal data may only be transferred when the transfer is occasional. It would have to be established on a case-by-case basis whether data transfers would be determined as “occasional” or “non-occasional”. In any case, this derogation can only be relied upon when the transfer is objectively necessary for the performance of the contract.

In relation to transfers necessary for important reasons of public interest (which must be recognized in EU or Member States⁶ law), the EDPB recalls that the essential requirement for the applicability of this derogation is the finding of an important public interest and not the nature of the organisation, and that although this derogation is not limited to data transfers that are “occasional”, this does not mean that data transfers on the basis of the important public interest derogation can take place on a large scale and in a systematic manner. Rather, the general principle needs to be respected according to which the derogations as set out in Article 49 GDPR should not become “the rule” in practice, but need to be restricted to specific situations and each data exporter needs to ensure that the transfer meets the strict necessity test.

9) Can I continue to use SCCs or BCRs to transfer data to another third country than the U.S.?

- The Court has indicated that SCCs as a rule can still be used to transfer data to a third country, however the threshold set by the Court for transfers to the U.S. applies for any third country. The same goes for BCRs.

The Court highlighted that it is the responsibility of the data exporter and the data importer to assess whether the level of protection required by EU law is respected in the third country concerned in order to determine if the guarantees provided by the SCCs or the BCRs can be complied with in practice. If this is not the case, you should assess whether you can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EEA, and if the law of the third country will not impinge on these supplementary measures so as to prevent their effectiveness.

⁵ See EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, adopted on 25 May 2018, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf, p.3.

⁶ References to “Member States” should be understood as references to “EEA Member States”.

You can contact your data importer to verify the legislation of its country and collaborate for its assessment. Should you or the data importer in the third country determine that the data transferred pursuant to the SCCs or to the BCRs are not afforded a level of protection essentially equivalent to that guaranteed within the EEA, you should immediately suspend the transfers. In case you do not, you must notify your competent SA⁷.

- ➔ Although, as underlined by the Court, it is the primary responsibility of data exporters and data importers to assess themselves that the legislation of the third country of destination enables the data importer to comply with the standard data protection clauses or the BCRs, before transferring personal data to that third country, the SAs will also have a key role to play when enforcing the GDPR and when issuing further decisions on transfers to third countries.

As invited by the Court, in order to avoid divergent decisions, they will thus further work within the EDPB in order to ensure consistency, in particular if transfers to third countries must be prohibited.

10) What kind of supplementary measures can I introduce if I am using SCCs or BCRs to transfer data to third countries?

- ➔ The supplementary measures you could envisage where necessary would have to be provided on a case-by-case basis, taking into account all the circumstances of the transfer and following the assessment of the law of the third country, in order to check if it ensures an adequate level of protection.

The Court highlighted that it is the primary responsibility of the data exporter and the data importer to make this assessment, and to provide necessary supplementary measures.

The EDPB is currently analysing the Court's judgment to determine the kind of supplementary measures that could be provided in addition to SCCs or BCRs, whether legal, technical or organisational measures, to transfer data to third countries where SCCs or BCRs will not provide the sufficient level of guarantees on their own.

- ➔ The EDPB is looking further into what these supplementary measures could consist of and will provide more guidance.

11) I am using a processor that processes data for which I am responsible as controller, how can I know if this processor transfers data to the U.S. or to another third country?

- ➔ The contract you have concluded with your processor in accordance with Article 28.3 GDPR must provide whether transfers are authorised or not (it should be borne in mind that even providing access to data from a third country, for instance for administration purposes, also amounts to a transfer).
- ➔ Authorization has also to be provided concerning processors to entrust sub-processors to transfer data to third countries. You should pay attention and be careful, because a large variety of computing solutions may imply the transfer of personal data to a third country (e.g., for storage or maintenance purposes).

⁷ See in particular recital 145 of Court's judgment . In relation to SCCs, see Clause 4(g) Commission Decision 2010/87/EU, as well as Clause 5(a) Commission Decision 2001/497/EC and Annex Set II (c) Commission Decision 2004/915/EC. In relation to BCRs, see Section 6.3 WP256 rev.01 (endorsed by the EDPB), and Section 6.3 WP257 rev.01 (endorsed by the EDPB).

12) What can I do to keep using the services of my processor if the contract signed in accordance with Article 28.3 GDPR indicates that data may be transferred to the U.S. or to another third country?

- ➔ If your data may be transferred to the U.S. and neither supplementary measures can be provided to ensure that U.S. law does not impinge on the essentially equivalent level of protection as afforded in the EEA provided by the transfer tools, nor derogations under Article 49 GDPR apply, the only solution is to negotiate an amendment or supplementary clause to your contract to forbid transfers to the U.S. Data should not only be stored but also administered elsewhere than in the U.S.
- ➔ If your data may be transferred to another third country, you should also verify the legislation of that third country to check if it is compliant with the requirements of the Court, and with the level of protection of personal data expected. If no suitable ground for transfers to a third country can be found, personal data should not be transferred outside the EEA territory and all processing activities should take place in the EEA.

For the European Data Protection Board

The Chair

Andrea Jelinek

Article 65 FAQ

How does cross-border cooperation work under the GDPR?

The General Data Protection Regulation (GDPR) requires the Supervisory Authorities (SAs) of the European Economic Area (EEA) to cooperate closely - under the umbrella of the [European Data Protection Board](#) (EDPB) - to ensure the consistent application of the GDPR and the protection of individuals' data protection rights across the EEA. One of their tasks is to coordinate decision-making in cross-border data processing cases.

A processing is cross-border when:

- data processing takes place in more than one country;
- or it substantially affects or it is likely to substantially affect individuals in more than one country.

Under the so-called one-stop-shop mechanism (Art. 60 GDPR), the Lead Supervisory Authority (LSA) acts as the main point of contact for the controller or processor for a given processing, while the Concerned Supervisory Authorities (CSAs) act as the main point of contact for individuals in the territory of their Member State. The LSA is the authority in charge of leading the cooperation process. It will share relevant information with the CSAs, carry out the investigations, prepare the draft decision relating to the case, and cooperate with the other CSAs in an endeavour to reach consensus on this draft decision.

What is the dispute resolution mechanism of Art. 65 GDPR?

When a Lead Supervisory Authority (LSA) issues a draft decision, it consults the Concerned Supervisory Authorities (CSAs), which can express their disagreement with the draft decision by submitting relevant and reasoned objections (RRO) within a period of four weeks (Art. 60 (4) GDPR).

When none of the CSAs objects, the LSA may proceed to adopt the decision.

In case at least one of the CSAs has expressed an RRO, and if the LSA intends to follow the objection, it shall submit a revised draft decision to all the CSAs. The CSAs then have a period of two weeks (Art. 60 (5) GDPR) to express their RROs to the revised draft decision.

However, if the LSA does not intend to follow the objection(s), since no consensus can be reached, the consistency mechanism is triggered. This means that the LSA is obliged to refer the case to the European Data Protection Board (EDPB) and the dispute resolution role of the EDPB is activated (Art. 65(1)(a) GDPR).

The dispute resolution mechanism can be triggered in two further cases:

- there is a disagreement as to which authority is the LSA (Art. 65(1)(b) GDPR);
- an SA does not seek the opinion of the EDPB as obliged under 64(1) GDPR or does not follow such an opinion (Art. 64(1) and (2) GDPR) (Art. 65(1)(c) GDPR).

What is the purpose of the dispute resolution mechanism of Art. 65(1)(a) and (b) GDPR?

The dispute resolution mechanism triggered under Art.65(1)(a) and (b) GDPR contributes to the good functioning of the cooperation mechanism by addressing any disagreements Concerned Supervisory Authorities (CSAs) may have in a given case or if there are conflicting views as to which authority is the Lead Supervisory Authority (LSA).

The EDPB will act as a dispute resolution body. It must adopt a decision to address the conflict between the involved SAs, which is binding on them (Art. 65 GDPR). The decision is adopted by a two-thirds majority of the members of the Board, and in case a decision cannot be adopted within 2 months, the decision is adopted within the next 2 weeks by a simple majority.

In which cases is the dispute resolution mechanism of Art. 65(1)(c) GDPR triggered?

While Art. 65 (a) and (b) relate to the one-stop-mechanism, Art.65(1)(c) GDPR concerns obligations of Supervisory Authorities (SAs)s stemming from the consistency mechanism.

More specifically, every competent SA has the duty to request an opinion from the EDPB before adopting national measures pursuant to article 64(1) GDPR. Such measures include lists of processing operations for which a Data Protection Impact Assessment (DPIA) is required, or the approval of a new set of standard clauses. In addition, under Art. 64(2) GDPR, any SA may also request an EDPB consistency opinion on any matter of general application or producing effects in more than one Member State.

If an SA does not request the opinion of the EDPB for the cases listed under Art. 64(1) GDPR or does not follow the EDPB opinion issued under Art. 64 GDPR, any SA and the European Commission can launch the dispute resolution procedure of Art. 65(1)(c) GDPR about the matter.

The dispute resolution mechanism of Art. 65 GDPR has been triggered - what happens next?

Within one month from the referral of the subject matter, the EDPB must adopt a decision by a two-thirds majority. The one-month deadline to adopt this binding decision can be extended by another month, if the case is complex. When the EDPB is not able to reach a decision within the abovementioned period, the decision must be adopted by a simple majority within two additional weeks. Should the members of the EDPB be split, the decision will be adopted by the vote of the EDPB Chair.

The EDPB has adopted its binding decision: when is it notified to the relevant national Supervisory Authorities (SAs) and in which language?

Once the EDPB has adopted a binding decision, the EDPB Chair notifies the binding decision to the relevant national SAs without undue delay.

Prior to the notification, the binding decision is translated into the languages of the relevant national SAs that have to adopt a final decision or take measures at national level on the basis

of the binding decision¹. Translation and proofreading can take a few weeks. In any case, the English version of the decision is the only authentic language version.

What is the next step for the relevant Supervisory Authorities (SAs)?

Once the relevant SAs have been notified of the binding decision, a decision has to be adopted at national level to implement the content of the binding decision. This decision will be adopted without undue delay and at the latest one month after the EDPB has notified its decision.

For cross-border cases where no consensus was found (Art. 65(1)(a) GDPR), the final decision will be addressed to the controller or processor and, where relevant, to the complainant.

When will the EDPB's decision be published in those cases where it settles conflicting views on a draft decision or where it decides on the Lead Supervisory Authority (LSA)?

Once the LSA or, in some cases the Concerned Supervisory Authority (CSA), with which the complaint was lodged has notified the EDPB of the date its final decision was communicated to the controller or processor and, where relevant, to the complainant, the EDPB will publish its own decision on its [website](#).

Can a Supervisory Authority (SA) challenge an Art. 65 GDPR decision by the EDPB?

As addressees of the EDPB decisions, the relevant SAs that wish to challenge these decisions can bring an action for annulment before the European Court of Justice (CJEU) within two months of being notified.

¹ Please see paragraphs 6 and 7 of Art. 11 of the EDPB Rules of Procedure. In exceptional cases, other CSAs can request, providing the reasons, an urgent translation in their official EU language(s) no later than at the moment of adoption of the binding decision.

How does the EDPB ensure harmonised data protection rights across 30 countries?

The EDPB has three main tasks:

- provide general guidance on the interpretation and application of EU data protection law;
- advise the European Commission on new legislation when it is of particular importance for the individuals' data protection rights and freedoms; and
- adopt consistency decisions and opinions on some national supervisory authorities' draft decisions having cross-border impact.



The European Data Protection Board (EDPB) is an independent EU body with a goal to bring about a consistent application of EU data protection law. The EDPB brings together the national Supervisory Authorities of all EU Member States and Iceland, Liechtenstein and Norway¹, and the data protection supervisor of the EU institutions (EDPS). The European Commission also has the right to participate in its works. In doing so, the EDPB helps to make sure that everyone in Europe enjoys the same data protection rights, no matter where they live.

1. As the GDPR has relevance also in those 3 countries, it covers the "EEA". Each time we refer to the "EU", it must be understood as "EEA", therefore also covering those 3 countries.



The EDPB: Guaranteeing the same rights for all

How the One-Stop-Shop works for you

Gianna, Pietro and Marco believe a private company has breached their data protection rights (and the rights of many other EU individuals) in a major way by sharing their personal data with third parties without any legal basis for doing so.

The group of individuals wish to complain about the company, however, they are all based across Italy, and the company's main establishment is located in Stockholm, Sweden.

Thankfully, the GDPR offers them the possibility to lodge a complaint with the Italian Data Protection Supervisory Authority.

Through the **one-stop-shop**, the Italian SA ("Concerned Supervisory Authority") can request the Swedish SA to investigate the complaint. As it is confirmed that many other individuals all across Europe are affected by the actions of the Swedish company, the Swedish SA takes up the role of "Lead Supervisory Authority".

The Swedish SA will cooperate with the Italian SA and every other competent authority. The Swedish SA will then come to a decision against the company. The Italian SA informs Gianna, Pietro and Marco in their own language of the decision that was issued by the Swedish SA.

However, if instead, the authorities concluded that the company did not breach the GDPR, the Italian SA will adopt a decision to dismiss or reject the complaint. If Gianna, Pietro and Marco disagree, they can – thanks to the one-stop-shop – challenge the decision reached by the Supervisory Authorities in front of a court in their Member State and thereby in their native language. Lastly, in case that the authorities cannot agree on an appropriate course of action - the Swedish SA will submit the matter to the EDPB. There, after the issue has been further analysed, the EDPB will vote to reach a binding decision that settles the dispute between the authorities.

The one-stop-shop helps individuals to stand up for their rights, no matter where they live in Europe.

General Guidance

The EDPB issues guidelines and recommendations to promote a common understanding of European data protection laws. The EDPB clarifies data protection provisions, and gives a uniform interpretation of rights and obligations.

Advisory Role to European Commission

The EDPB advises the European Commission on any issue related to the protection of personal data and newly proposed legislation with an important impact on data protection rights and obligations. By doing so, the EDPB makes sure that new EU legislation upholds the highest standards of data protection.

Consistency & One-Stop-Shop

Under the GDPR, enforcement is the responsibility of the national supervisory authorities (SAs). Each EU Member State has its own independent supervisory authority, which oversees the application of the GDPR, including the handling of complaints. For data processing taking place in multiple EU countries, the GDPR provides a system of cooperation between the competent SAs, within which they cooperate in order to reach consensus. This **one-stop-shop** mechanism is designed to reduce the administrative burden for organisations and make it simpler for individuals to exercise their rights from their home base.



Letters



Access Now
Amnesty International
Asociatia pentru Tehnologie si Internet (ApTI)
Bits of Freedom
Digitalcourage
Digitale Gesellschaft
Državljan D
Electronic Frontier Finland
European Center for Not-for-Profit Law Stichting (ECLN)
European Digital Rights (EDRi)
Fitug e.V.
Homo Digitalis
IT-Pol Denmark
La Quadrature du Net
noyb
Open Rights Group
Panoptikon
Privacy International

Brussels, 14/06/2022

Ref: OUT2022-0046

Dear Madam/ Sir,

The EDPB very much welcomes your letter calling upon the structural and procedural enforcement of the GDPR and its work to promote and safeguard data protection.

It has always been in focus of our activities to further enhance the effectiveness of cooperation and enforcement procedures under the GDPR, as evidenced by the statistics on the Supervisory Authorities' activities in 2021: 505 cross-border cases have been created in the case register, 209 One-stop-shop (Art 60) draft decisions have been issued, which resulted in 141 Final Decisions.

To improve the cooperation between data protection supervisory authorities, the Board has already launched several initiatives, such as the Coordinated Enforcement Framework, the Support Pool of Experts, or Secondment programmes, which would facilitate the sharing of knowledge, exchange of experts, methodologies and good practices among the authorities, with the active participation of colleagues from the authorities. I would also like to recall the guidance recently published by the EDPB

regarding OSS procedures (Guidelines 02/22), which addresses several key cooperation issues in order to outline legally sound and consistent approaches to be followed by all SAs and the new Guidelines on the calculation of administrative fines under the GDPR (Guidelines 04/2022).

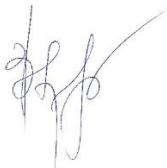
A two-day high level meeting took place in Vienna in April 2022, where the EDPB members agreed to diversify the cooperation methods used for strong and swift enforcement and consistent interpretation and application of the GDPR. In this context the EDPB members agreed:

- i. to collectively identify cross border cases of strategic importance in different Member States on a regular basis, for which cooperation will be prioritised and supported by EDPB;
- ii. that the EDPB will deal with specific legal issues on matters of general application for instance by making greater use of consistency opinion to take position;
- iii. that they commit to further exchange information on national enforcement strategies with a view to agreeing on annual enforcement priorities at EDPB level;
- iv. to facilitate the cross-border exchange of information, and therefore propose a template for data subjects' complaints, to be used by DPAs on a voluntary basis, and to improve IT cooperation tools of the EDPB;
- v. to identify a list of procedural aspects that could be further harmonised in EU law to maximise the positive impact of GDPR cooperation; and
- vi. to solidly embed the GDPR and DPAs in the overall regulatory architecture that is being developed for the digital market (Data Act, DMA, DSA, AI Act, DGA).

Regarding EDRI's call for guidance for DPAs, the EDPB acknowledges that different procedural rules, different data protection cultures and different market situations pose challenges for the consistent application of the GDPR, however one of the EDPB's main objectives is to bridge these differences and provide guidelines for consistent application.

Overall, the GDPR has created an innovative governance system designed to ensure a high level of data protection and the EDPB members are fully committed to the consistent and effective application of the GDPR.

Yours sincerely,



Ventsislav Karadjov

Vice-Chair of the EDPB

Note



Final

6th meeting of the Coordinated Supervision Committee

6 July 2022, Hybrid

Summary

The Coordinated Supervision Committee (“the Committee”) met on 6 July 2022 in hybrid format with some of its members participating remotely and others in person.

[Europol](#)

The Committee discussed the recent entry into operation of the amendments to the Europol Regulation. It underlined their impact on matters relevant to data protection such as purpose limitation, data storage, rights of access and data subject categorisation. The Committee decided to include some activities in its Work Programme 2022-2024 in this connection, such as inspecting the lawfulness of the processing of data transferred to Europol on minors; addressing the so called Europol “big data challenge”; following closely the determination of the purposes of the data processing by national competent authorities and by Europol under Articles 18 and 19 of the Europol Regulation; and monitoring the implementation of the new possibility for Europol to propose to Members issuing alerts in SIS.

The Committee noted that Europol will have access to personal data stored in several information systems such as VIS, Eurodac, SIS and others. The Committee will use its horizontal and holistic approach to address the issues resulting from these multiple accesses, taking into account that the accessed data will be entered into these systems at national level.

[European Public Prosecutor’s Office \(EPPO\)](#)

The Committee discussed initiatives to obtain additional information for itself and its members with the information systems the EPPO will be using and its interactions with national databases. Information will be exchanged between its members in this regard and visits to some authorities possibly organised in the future.

[Internal Market Information System \(IMI\)](#)

The Committee continued its discussions on how to improve the information available to data subjects on how to exercise their rights in relation to the processing of their personal data in the IMI. The Committee discussed the preparation of recommendations to competent authorities acting as

controllers to raise their awareness of their information obligations under the GDPR and provide them with guidance on how to fulfil them.

[CSC Work Programme 2022-2024](#)

The Committee adopted its Work Programme for the period 2022-2024.

[Joint biannual report of activities on coordinated supervision \(Art. 10 CSC RoP\)](#)

The Committee adopted its joint biannual report of activities on coordinated supervision for the period 2020-2022.

Note



Final

7th meeting of the Coordinated Supervision Committee

30 November 2022, Hybrid

Summary

The Coordinated Supervision Committee (“the Committee”) met on 30 November 2022 in hybrid format with some of its members participating remotely and others in person.

IMI

The Committee discussed its ongoing work on the preparation of draft recommendations to competent authorities on the information to be provided to data subjects for the exercise of their rights over the processing of their personal data in the IMI system.

Europol

The EDPS informed the Committee of its recent request for annulment of Articles 74(a) and 74(b) of the newly amended Europol Regulation that it filed before the CJEU on 16 September 2022. The EDPS considers that the retroactive effect of these provisions, which legalise Europol’s practice of processing large volumes of individuals’ personal data with no established link to criminal activity, affects its independence and its institutional prerogatives. The EDPS had enforced its powers by issuing an order on 3 January 2022 requesting Europol to delete the concerned datasets within a predefined and clear time limit.

Within the implementation of its working programme, the Committee discussed to take coordinated action to check how Articles 74(a) and 74(b) of the Europol Regulation are implemented at national level and national procedural safeguards complied with.

The implementation of Article 18a - “Processing of personal data in support of a criminal investigation” of the recast of the Europol Regulation and the exercise of data subject rights in this regard were also addressed.

The EDPS provided also information to the Committee on the data subject complaints on Europol’s processing of their personal data, and on the prior consultations received from Europol on different forms of data processing.

The Committee also discussed the processing of personal data on minors by Europol and the actions to be taken in this respect at national and European levels to ensure that this processing complies with the Europol Regulation and national law.

The Committee decided to work on updating the guide for the exercise of data subject rights in Europol, based on the recast of the Europol Regulation.

[European Public Prosecutor's Office \(EPPO\)](#)

The EDPS informed the Committee of its visit of the EPPO, its views on the EPPO case management system, and the efforts the EPPO is making to comply with the applicable data protection regulations.

The Committee discussed the organisation of joint visits of the EDPS and national supervisory authorities to the European Delegated Prosecutors operating in each Member State to obtain additional information on their processing of personal data.

[Eurojust](#)

The Committee covered Eurojust's implementation of its new mandate to support Member States' action in combating genocide, crimes against humanity, war crimes and related criminal offences and the information systems and secure channels that Eurojust uses and will use to this end.

The Committee also discussed about the processing of personal data in the joint investigation teams that Eurojust facilitates. It focused especially on the data protection safeguards that may be required in joint investigation teams formed with third countries' authorities.

The Committee discussed the implementation of a fact-finding exercise at national level on the processing of data in the Eurojust counter-terrorism register.

[Interoperability](#)

The Committee received an update from the European Commission on the entry into operation of the EU large-scale information systems covered by the EU interoperability regulations (SIS, VIS, EES, ETIAS, Eurodac, ECRIS-TCN) and the technical features of their interoperability. The Committee exchanged with the European Commission on aspects such as the verification of the identity matches.

[Election of the CSC Coordinator](#)

The Committee re-elected the incumbent CSC Coordinator, Ms. Clara Guerra, from the Portuguese supervisory authority, for an additional term of two years.

[AOB](#)

The Committee was informed of the Supervision Conference on data protection and criminal justice, held on 29 November by the EDPS, Eurojust and the EPPO.

Note



Final

8th meeting of the Coordinated Supervision Committee

22 March 2023, Hybrid

Summary

The Coordinated Supervision Committee (“the Committee”) met on 22 March 2023 in hybrid format with some of its members participating remotely and others in person.

CSC Organisational Issues

The Committee discussed the future organisation of the meeting, member participation and Confluence structure.

SIS

The Committee discussed the handover from the SIS II SCG to the CSC.

The Committee then agreed that its members could still provide their responses to the Art. 36 alerts questionnaire by the end of May 2023.

The Committee adopted an updated version of the Schengen Guide for exercising Data Subject Rights, and agreed to its publication in the CSC website.

A drafting team was initiated to assess the legal interpretation of Supervisory Authority’s requirement to carry out an audit of SIS.

The Committee agreed to coordinate the monitoring, from the outset, of the new SIS Article 40 alerts on unknown wanted persons for the purposes of identification under national law, which contain dactyloscopic data collected at serious crime scenes.

Eurojust

The Committee discussed the processing of personal data in the joint investigation teams involving third countries, based on information gathered at national level.

The Committee also discussed the supervision of Eurojust at a national level and it was agreed that further input from members was needed to prepare an analysis on the issue.

[Europol](#)

The Committee discussed the processing of personal data on minors in Europol and the members agreed to continue checking at national level the contributions of Members States' authorities to Europol, based on the information provided by the EDPS. The results of the verifications which had already been made at national level were discussed by the Committee. The Committee decided to discuss some guidelines at the next CSC meeting to better assist EDPS in their engagement with Europol in this matter.

[AOB](#)

The EDPS asked the Committee to share any feedback from their previous experience of auditing the IMI system.

The Committee was informed of a planned operational visit to the European delegated prosecutors at national level to be coordinated between the EDPS and the respective national Supervisory Authority, under Article 87 of the EPPO Regulation.

The Committee discussed the management of supervising all the new large scale IT systems. Some Supervisory Authorities are taking concrete initiatives, including by commissioning studies on the matter, to address their supervisory role in the near future, also looking at a multidisciplinary approach regarding allocating responsibilities for supervision and allocating resources. The Committee agreed to continue this discussion and actively contribute to this debate.

Minutes

Final

9th meeting of the Coordinated Supervision Committee (CSC)

14 June 2023, Physical

Summary

The Coordinated Supervision Committee ("the Committee") met on 14 June 2023 physically.

Item 1: Welcome and Introduction

The agenda was adopted. The minutes and the summary of discussions of 8th CSC meeting were adopted.

Item 2: General Issues

The Committee exchanged on the workshop on strategies for supervision of the EU information systems organised by NL SA tentatively in September. The purpose of the workshop is to exchange experiences and ideas on how DPAs are addressing, in terms of organisation and intervention, their supervisory tasks vis-à-vis the enlargement of EU information systems, cross access rights and data flows and interoperability.

The Coordinators reminded the members that one of the activities of the CSC Working Programme (2023-2024) is to engage actively with civil society. They proposed to have a kick off meeting with NGOs as guests, at the next CSC physical meeting. There was a first exchange of views on the approach and on the format to be followed. Members were asked for further input for a proposal to be presented in the September meeting.

Item 3: Border, asylum and migration

The Coordinator noted that Cyprus integration is expected in July 2023.

The eu-LISA DPO had sent written input, which was shared with the members. The Committee took note of the enhanced capabilities of the SIS, as well as of the statistics on the new Article 40 alerts.

The CSC SEC provided an update on the number of replies received on Article 36 SIS questionnaire, and it will start compiling the input.

The Committee further discussed and adopted a draft model letter to be sent to competent authorities for collection of statistics on Data Subjects' Rights (DSR), pursuant to Article 54(3) of Regulation (EU) 2018/1861 and Article 68(3) of Regulation (EU) 2018/1862, highlighting the need to use the template adopted by the Commission through an Implementing Act and advising to better prepare to collect and structure the statistical data required in a way that facilitates later on the provision of such figures in a compliant manner. The statistics should be sent to the EDPB, after consolidation at national level. The Committee referred briefly to its ongoing work on the audit cycle standards.

The Committee also discussed the case where a person submits an access request to the SIS addressed simultaneously to several authorities in several countries and how this situation should be handled.

3.2 European Travel Information and Authorisation System (ETIAS)

The Deputy Coordinator provided a brief report on the ETIAS Fundamental Rights Guidance Board (EFRGB). The tasks of the central unit concern how to interpret the audit, with the support of the EFRGB.

In terms of internal organisation, there is a need to be present at the working groups meetings, to develop recommendations for the assessment of the screening rules on the impact of fundamental rights and discrimination. The Committee discussed the important role of ETIAS national units in the system, in terms of controllership for this part of the processing, and the need to carry out national data protection impact assessments (DPIA).

Item 4 : Digital single Market (IMI)

The rapporteurs thanked the members for their input on the recommendations on transparency obligations and noted that they need more time to finalise it.

Item 5: Police and judicial cooperation

The rapporteur presented the updated draft guide for the exercise of data subjects' rights in relation to Europol. The updated version includes more references to Regulation 2018/1725 and consolidates different texts.

The EDPS made a presentation on the use of Europol Information Systems (EIS) for cross-checking information purposes, under Art. 18(2) (a) of the Europol Regulation. The Committee also took note of two EDPS opinions related to the National Center for Missing and Exploited Children (NCMEC) reports and QUEST+.

The Committee discussed the coordinated supervisory activity on the lawfulness of the transmission of minors' data from Member States to Europol, and took note of the update provided by members.

The EDPS informed the Committee about the audit to the EPPO that took place in April 2023 in Luxembourg.

The next CSC meeting will be held, remotely, on the 7 September 2023.



Coordinated
Supervision
Committee



EUROPOL'S INFORMATION SYSTEMS

A GUIDE FOR EXERCISING DATA SUBJECTS' RIGHTS: THE RIGHT OF ACCESS, RECTIFICATION, ERASURE AND RESTRICTION

This guide was compiled by the Coordinated Supervision Committee.

The national contributions, and any translations of this guide into languages other than English, are the responsibility of each national supervisory authority and they do not necessarily reflect the official position of the CSC. The CSC does not guarantee the accuracy of the information included in the national contributions and any questions should be addressed to the respective national supervisory authorities. Neither the CSC nor any person acting on the CSC's behalf may be held responsible for the use which may be made of the information contained therein.

Secretariat postal address: Rue Wiertz 60, B-1047 Brussels

Offices: Rue Montoyer 30, B-1000 Brussels

E-mail : csc-secretariat@edpb.europa.eu

TABLE OF CONTENTS

1. DATA CATEGORIES AND EXCHANGE OF PERSONAL DATA BETWEEN MEMBER STATES AND EUROPOL.....	5
2. RIGHTS GRANTED TO INDIVIDUALS WHOSE DATA ARE PROCESSED BY EUROPOL.....	7
2.1. Right of access.....	8
2.2. Right to rectification, erasure and restriction	9
2.3. Right to have the legality of data relating to them transferred to Europol verified	10
2.4. Remedies: the right to complain to EDPS or to initiate a judicial proceeding.....	10
3. CONTACT POINTS.....	11
3.1. AUSTRIA	12
3.2. BELGIUM	12
3.3. BULGARIA.....	12
3.4. CROATIA.....	13
3.5. CYPRUS.....	13
3.6. CZECH REPUBLIC.....	14
3.7. ESTONIA.....	14
3.8. FINLAND.....	15
3.9. FRANCE	15
3.10. GERMANY.....	16
3.11. GREECE.....	16
3.12. HUNGARY.....	17
3.13. IRELAND	17
3.14. ITALY	18
3.15. LATVIA.....	18
3.16. LITHUANIA.....	19
3.17. LUXEMBOURG.....	19
3.18. MALTA.....	20

3.19. NETHERLANDS	20
3.20. POLAND.....	21
3.21. PORTUGAL.....	21
3.22. ROMANIA.....	21
3.23. SLOVAK REPUBLIC.....	22
3.24. SLOVENIA	23
3.25. SPAIN	23
3.26. SWEDEN	24
ANNEXES (TEMPLATE LETTERS)	25
Annex 1	25
Annex 2	26

Individuals whose personal data are collected, held or otherwise processed by Europol are entitled to rights regarding their personal data, namely the right of access, right to rectification, erasure and restriction of personal data and the right to have the legality of transfer of his or her personal data verified by a national supervisory authority.

This Guide describes the modalities for exercising those rights.

The Guide is divided into three sections: (I) data categories and exchange of personal data between Member States and Europol, (II) the rights granted to the individuals whose personal data are processed in Europol's Information Systems and (III) a description of the procedure for exercising the right of access in each of the countries concerned.

1. DATA CATEGORIES AND EXCHANGE OF PERSONAL DATA BETWEEN MEMBER STATES AND EUROPOL

Europol processes personal data based on Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) (hereinafter "Europol Regulation"), as amended by Regulation 2022/991 of the European Parliament and of the Council of 8 June 2022 (hereinafter "Regulation amending Europol Regulation").

Categories of personal data processed

Personal data collected and processed by Europol relate to:

- a) persons who, in accordance with the national law of the Member State concerned, are suspected of having committed or having taken part in a criminal offence in respect of which Europol is competent, or who have been convicted of such an offence;
- b) persons regarding whom there are factual indications or reasonable grounds under the national law of the Member State concerned to believe that they will commit criminal offences in respect of which Europol is competent;
- c) persons who might be called on to testify in investigations in connection with the offences under consideration or in subsequent criminal proceedings;

- d) persons who have been the victims of one of the offences under consideration or with regard to whom certain facts give reasons to believe that they could be the victims of such an offence;
- e) contacts and associates; and
- f) persons who can provide information on the criminal offences under consideration.

The categories of personal data and categories of data subjects whose data may be collected and processed for each purpose referred to in Article 18(2) are listed in Annex II to the Europol Regulation¹.

Processing of personal data, by automated or other means, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership and processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, or data concerning a person's health or sex life shall be allowed only where strictly necessary and proportionate for the purposes of research and innovation projects pursuant to Article 33a and for operational purposes, within Europol's objectives, and only for preventing or combating crime that falls within Europol's objectives. Such processing shall also be subject to appropriate safeguards laid down in this Regulation with regard to the rights and freedoms of the data subject, and, with the exception of biometric data processed for the purpose of uniquely identifying a natural person, shall be allowed only if those data supplement other personal data processed by Europol.

The selection of a particular group of persons solely on the basis of such personal data shall be prohibited.

Exchange of personal data

Europol should be a hub for information exchange in the Union. Information collected, stored, processed, analysed and exchanged by Europol includes criminal intelligence which relates to information about crime or criminal activities falling within the scope of Europol's objectives, obtained with a view to establishing whether concrete criminal acts have been committed or may be committed in the future.

¹ Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, page 57

In order to ensure an effective cooperation between Europol and Member States, a national unit should be set up in each Member State. The national unit should be the liaison link between national competent authorities and Europol. To ensure a continuous and effective exchange of information between Europol and the national units, and to facilitate their cooperation, each national unit should designate at least one liaison officer to be attached to Europol. The liaison officers shall assist in the exchange of information between Europol and their Member States.

Also, liaison officers shall assist in the exchange of information between their Member States and the liaison officers of other Member States, third countries and international organisations.

2. RIGHTS GRANTED TO INDIVIDUALS WHOSE DATA ARE PROCESSED BY EUROPOL

In accordance with data protection principles, all individuals whose data are processed by Europol are granted specific rights by the aforementioned Europol Regulation.

These are basically:

- the right of access to data relating to them stored by Europol;
- the right to rectification, erasure and restriction;
- the right to have the legality of data relating to them transferred to Europol verified;
- the right to bring proceedings before the court or competent authorities to correct or delete data or to obtain compensation.

Anyone exercising any of these rights can apply to the authority appointed for that purpose in the Member State of his or her choice. That authority shall refer the request to Europol without delay and in any case within one month of receipt.

Deadlines for replies to individuals' requests

When an individual exercises his/her right of access, his/her right to rectification, erasure and restriction, Europol shall answer it without undue delay, and in any case within three months of receipt by Europol of the request from the national authority.

2.1. Right of access

The right of access is the possibility for anyone who so requests to consult the information relating to him/her stored in a data file. This is a fundamental principle of data protection which enables data subjects to exercise control over personal data which is being processed by the controller, namely by Europol.

This right is expressly provided for in Article 36 of Europol Regulation, and Article 80 of Regulation (EU) 2018/1725.

Any data subject wishing to exercise the right of access to personal data relating to him or her may make a request to that effect to the authority appointed for that purpose in the Member State of his or her choice, or to Europol. Where the request is made to that authority, it shall refer the request to Europol without delay and in any case within one month of receipt.

Europol shall answer it without undue delay and in any case within three months of receipt by Europol of the request from the national authority.

Europol shall consult the competent authorities of the Member States and the provider of the data concerned so that they could have the opportunity to state their position as to the possibility of disclosing the data to the applicant, and to object to Europol's proposed response. In the latter case, the Member State or the provider of the data concerned shall notify Europol of the reasons for its objection.

According to Article 81 of Regulation (EU) 2018/1725, Europol may restrict, wholly or partly, the right of access of the extent that, and for as long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned, in order to:

- a) avoid obstructing official or legal inquiries, investigations or procedures;
- b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- c) protect the public security of Member States;
- d) protect the national security of Member States;
- e) protect the rights and freedoms of others, such as victims and witnesses.

In the cases referred above, Europol shall inform the data subject, without undue delay, in writing of any refusal or restriction of access and of the reasons for the refusal or the restriction. Such

information may be omitted where the provision thereof would undermine one of the purpose above.

2.2. Right to rectification, erasure and restriction

Besides the right of access, there is also the right to request Europol, through the authority appointed for that purpose in the Member State of his or her choice, or to Europol, to rectify personal data concerning him or her held by Europol if they are incorrect or to complete or update the personal data.

The data subjects have also the right to request Europol, directly or through the authority appointed for that purpose in the Member State of his or her choice, to erase personal data relating to him or her held by Europol if they are no longer required for the purposes for which they are collected or are further processed.

If there are reasonable grounds to believe that erasure could affect the legitimate interests of the data subjects, Europol shall restrict rather than erase personal data. Restricted data shall be processed only for the purpose of protecting the rights of the data subject, where it is necessary to protect the vital interests of the data subject or of another person, or for the purposes laid down in Article 82(4) of Regulation (EU) 2018/1725 and listed below:

- a) avoid obstructing official or legal inquiries, investigations or procedures;
- b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- c) protect the public security of Member States;
- d) protect the national security of Member States;
- e) protect the rights and freedoms of others, such as victims and witnesses.

In all the cases, where the request is made to that authority, it shall refer the request to Europol without delay and in any case within one month of receipt.

If personal data held by Europol have been provided to Europol by third countries, international organisations or Union bodies, have been directly provided by private parties, have been retrieved by Europol from publicly available sources or result from Europol's own analyses, Europol shall rectify or erase such data or restrict their processing and when appropriate, inform the providers of the data.

If personal data held by Europol have been provided to Europol by Member States, the Member States concerned shall rectify or erase such data or restrict their processing in collaboration with Europol, within their respective competences.

The data subject shall be informed in writing of any refusal of rectification, erasure or restricting, of the reasons for such a refusal and of the possibility of lodging a complaint with the EDPS and of seeking a judicial remedy.

2.3. Right to have the legality of data relating to them transferred to Europol verified

Article 42 (4) of the Europol Regulation provides for the right to request the national supervisory authority of a Member State to verify the legality of any transfer or communication to Europol of data concerning him or her and of access to those data by the Member State concerned.

Data subjects may request this verification in the Member State in which they wish for their right to be exercised.

The right to request verification shall be exercised in accordance with the national law of the Member State in which the request is made.

The national supervisory authority shall carry out the requested action by verifying whether the transfer of data to Europol by national competent authorities was done in a lawful way and shall communicate the outcome of the action to the data subject, all according to rules of national law.

Article 84 of the Regulation (EU) 2018/1725 provides that this right can also be exercised through the European Data Protection Supervisor (EDPS) in cases where Europol may delay, restrict or omit the provision of the information to data subjects (according to Article 79(3) of this Regulation), or limit the right to access (according to Article 81) or refuse to rectify or erase data (according to Article 82(4)). The EDPS shall at least inform the data subject that all necessary verifications or a review by him or her have taken place, and of his or her right to seek a judicial remedy before the Court of Justice.

2.4. Remedies: the right to complain to EDPS or to initiate a judicial proceeding

Articles 47 and 50 of Europol Regulation present the remedies accessible to individuals when their request has not been satisfied.

Any person may bring an action against Europol before the Court of Justice of the European Union, or against the Member State before a competent national court of that Member State to receive compensation for damage suffered.

Any data subject shall have the right to lodge a complaint with the EDPS if he or she considers that the processing by Europol of personal data relating to him or her does not comply with the Europol Regulation or Regulation (EU) 2018/1725. The EDPS shall inform the data subject of the progress and outcome of the complaint, as well as the possibility of a judicial remedy.

Additional information on the data protection supervisory role of the EDPS over Europol are to be found on the website of the EDPS within the dedicated section on “Supervision of Europol” (https://edps.europa.eu/data-protection/our-role-supervisor/supervision-europol_en).

3. CONTACT POINTS

The contact details of the body to which requests for access, rectification or erasure should be addressed, if not directly to Europol, are **provided in the remainder of this chapter, together with the contact details of the data protection authorities of each Member State and the EDPS.**

3.1. AUSTRIA

1. Contact details of the body to which requests for access, rectification or erasure should be addressed

Büro 2.2 Nationale Stelle EUROPOL
Josef-Holaubek-Platz 1, 1090 Wien,
email: BMI-II-BK-2-2@bmi.gv.at

2. Contact details of the national data protection authority

Österreichische Datenschutzbehörde
Barichgasse 40-42, 1030 Wien
Tel: +43 1 52 152-0
email: dsb@dsb.gv.at

3.2. BELGIUM

Contact details of the body to which requests for access, rectification or erasure should be addressed and police dedicated national data protection authority

Controleorgaan op de politieonele
informatie/Organe de contrôle de
l'information policière
Leuvenseweg/Rue de Louvain 48
1000 Brussel/Bruxelles
België/Belgique
Tel: +32 2 549 94 20
email : info@controleorgaan.be /
info@organedecontrole.be
Website: <https://www.controleorgaan.be> /
<https://www.organedecontrole.be>

Police processing monitoring:
Controleorgaan op de politieonele
informatie/Organe de contrôle de l'information
policière

3.3. BULGARIA

1. Contact details of the body to which requests for access, rectification or erasure should be addressed

Ministry of Interior
29, Shesti Septemvri Str.
1000 SOFIA
Tel: +359 2 9825 000
email: priemna@mvr.bg

Website: <https://www.mvr.bg/>

2. Contact details of the national data protection authority

Commission for Personal Data Protection

2, Prof. Tsvetan Lazarov blvd.

Sofia 1592

Tel: + 359 2 915 3519

Fax: +359 2 915 3525

email: kzld@cpdp.bg

Website: <https://www.cpdp.bg/>

3.4. CROATIA

1. Contact details of the body to which requests for access, rectification or erasure should be addressed

Ministry of the Interior

Ulica grada Vukovara 33

HR - 10 000 Zagreb

email: pitanja@mup.hr

Website: www.mup.hr

2. Contact details of the national data protection authority

Croatian Personal Data Protection Agency

Selska cesta 136

10000 Zagreb

Tel: +385 1 4609 000

Fax: +385 1 4609 099

email: azop@azop.hr

Website: [http://www.azop.hr/](http://www.azop.hr)

3.5. CYPRUS

1. Contact details of the body to which requests for access, rectification or erasure should be addressed

Chief of Police

(for EUROPOL National Unit),

Antistratigou Evangelou Floraki Street,

Police Headquarters,

1478 Nicosia, Cyprus

e-mail: cyeuropol@police.gov.cy

2. Contact details of the national data protection authority

Commissioner for Personal Data Protection

15 Kypranoros Street

1061 Nicosia

P.O. Box 23378, CY-1682 Nicosia
Tel: +357 22 818 456
Fax: +357 22 304 565
email: commissioner@dataprotection.gov.cy
Website: <http://www.dataprotection.gov.cy/>

3.6. CZECH REPUBLIC

1. Contact details of the body to which requests for access, rectification or erasure should be addressed

Policie České republiky
Policejní prezidium ČR
Strojnická 27
170 89 Praha 7
Česká republika
email: epodatelna.policie@pcr.cz
website: www.policie.cz

2. Contact details of the national data protection authority

Úřad pro ochranu osobních údajů
Pplk. Sochora 27
170 00 Praha 7
Česká republika
email: posta@uouu.cz
website: www.uouu.cz

3.7. ESTONIA

1. Contact details of the body to which requests for access, rectification or erasure should be addressed

Europol National Unit
Police and Border Guard Board
Pärnu mnt 139, 15060 Tallinn, Estonia
email: ppa@politsei.ee
Website: <https://www.politsei.ee/en/>

2. Contact details of the national data protection authority

Estonian Data Protection Inspectorate
(Andmekaitse Inspektsioon)
Tatari 39
10134 Tallinn
Tel. +372 6274 135
email: info@aki.ee
Website: <http://www.aki.ee/>

3.8. FINLAND

1. Contact details of the body to which requests for access, rectification or erasure should be addressed

Central Criminal Police
Jokiniemenkuja 4
PL 285
FIN-01301 Vantaa
Suomi/Finland
email: kirjaamo.keskusrikospoliisi@poliisi.fi

2. Contact details of the national data protection authority

Office of the Data Protection Ombudsman
Lintulahdenkuja 4
P.O. Box 800
FIN-00531 Helsinki
Suomi/Finland
Tel: +358 29 566 6700
email: tietosuoja@om.fi
Website: <http://www.tietosuoja.fi/en/>

3.9. FRANCE

1. Contact details of the body to which requests for access, rectification or erasure should be addressed

Commission Nationale de l'Informatique et
des Libertés (CNIL)
3 Place de Fontenoy
TSA 80715 - 75334 Paris CEDEX 07
France
Tel: +33 1 53 73 22 22
Website: <http://www.cnil.fr>

2. Contact details of the national data protection authority

Commission Nationale de l'Informatique et des
Libertés (CNIL)
3 Place de Fontenoy
TSA 80715 - 75334 Paris CEDEX 07
France
Tel: +33 1 53 73 22 22
Website: <http://www.cnil.fr>

3.10. GERMANY

1. Contact details of the body to which requests for access, rectification or erasure should be addressed

Bundeskriminalamt
65173 Wiesbaden
Germany
email: ds-petenten@bka.bund.de

2. Contact details of the national data protection authority

Federal Commissioner for Data Protection and
Freedom of Information
Graurheindorfer Str. 153
53117 Bonn
Germany
Tel: +49 228 997799 0
email: poststelle@bfdi.bund.de
De-mail: poststelle@bfdi.de-mail.de
Website: <https://www.bfdi.bund.de>

3.11. GREECE

1. Contact details of the body to which requests for access, rectification or erasure should be addressed

Ministry of Citizen Protection
Hellenic Police HQ
International Police Cooperation Division
Europol National Unit
4, P. Kanellopoulou Street
101 77, Athens
Greece
Tel. 1: +30210 69 842 86
Tel. 2: 213 1520334
email: europol@police.gr

2. Contact details of the national data protection authority

Hellenic Data Protection Authority
Kifisia Av. 1-3, PC 11523
Ampelokipi Athens
Greece
Tel: +30210 64 75 600
Fax: +30210 64 75 628
email: contact@dpa.gr
Website: <http://www.dpa.gr/>

3.12. HUNGARY

1. Contact details of the body to which requests for access, rectification or erasure should be addressed

National Police Headquarters
International Law Enforcement Cooperation
Centre
Address: H-1139 Budapest, Teve u. 4-6
Postal address: H-1903 Budapest, Pf.: 314/15
Tel: +36 1 443 5596
Fax: +36 1 443 5815
email: nebek@nebek.police.hu
Website: <http://www.police.hu>

2. Contact details of the national data protection authority

National Authority for Data Protection and
Freedom of Information
H-1055 Budapest, Falk Miksa u.9-11.
Postal address: H-1363 Budapest, Pf.:9
Tel: +36 1 391 1400
email: ugyfelszolgalat@naih.hu
Website: <http://www.naih.hu>

3.13. IRELAND

1. Contact details of the body to which requests for access, rectification or erasure should be addressed

Europol National Unit
Liaison & Protection
Garda Headquarters
Phoenix Park
Dublin 8
Tel: +353 1 666 0000
Website: <http://www.garda.ie>

2. Contact details of the national data protection authority

Data Protection Commission
21 Fitzwilliam Square,
Dublin 2,
D02 RD28,
Ireland
Phone: +353 (01) 7650100
E-mail: info@dataprotection.ie
Website: www.dataprotection.ie

3.14. ITALY

1. Contact details of the body to which requests for access, rectification or erasure should be addressed

Unità Nazionale Europol
c/o Direzione Centrale della Polizia Criminale – Servizio per la Coop.ne Int.le di Polizia
Via Torre di Mezzavia, 9
00173 Roma – Italy

2. Contact details of the national data protection authority

Garante per la Protezione dei Dati Personalni
Piazza di Monte Citorio 121
I-00186 Roma
Italia
Tel. +39 06 69677 1
Fax +39 06 69677 3785
email: garante@garanteprivacy.it
Website: <http://www.garanteprivacy.it/>

3.15. LATVIA

1. Contact details of the body to which requests for access, rectification or erasure should be addressed

Data State Inspectorate
Elias Street 17,
LV 1050 Riga
Tel: +371 6722 3131
email: pasts@dvi.gov.lv
Website: <http://www.dvi.gov.lv/>

2. Contact details of the national data protection authority

Data State Inspectorate
Elias Street 17,
LV 1050 Riga
Tel: +371 6722 3131
email: pasts@dvi.gov.lv
Website: <http://www.dvi.gov.lv/>

3.16. LITHUANIA

1. Contact details of the body to which requests for access, rectification or erasure should be addressed

International Liaison Office of Lithuanian
Criminal Police Bureau,
Saltoniskiu St. 19
LT-08105 Vilnius
Tel.: +370 5 2719900
Fax.: +370 52719924
email: trv@policija.lt
Website: www.policija.lt

2. Contact details of the national data protection authority

State Data Protection Inspectorate
Sapiegos Str. 17
LT-10312 Vilnius
Tel: + 370 5 279 14 45
email: ada@ada.lt
Website: <https://vdai.lrv.lt>

3.17. LUXEMBOURG

1. Contact details of the body to which requests for access, rectification or erasure should be addressed

Direction Générale de la Police Grand-Ducale
A l'attention du délégué à la protection des données
Cité Policière Grand-Duc Henri,
B.P. 1007
L-2957 Luxembourg
Email : dpo@police.etat.lu
Website: <https://police.public.lu/fr/support/protection-des-donnees-a-caractere-personnel.html>

2. Contact details of the national data protection authority

Commission Nationale pour la Protection des Données
15, boulevard du Jazz
L-4370 Belvaux
Tel: +352 2610 60 1
Fax: +352 2610 60 29
email: info@cnpd.lu
Website: <http://www.cnpd.lu>

3.18. MALTA

1. Contact details of the body to which requests for access, rectification or erasure should be addressed

The Data Protection Officer

Legal Unit

Police Headquarters

St. Calcedonius Square

Floriana FRN 1530

Tel: +35621224001

Website: www.pulizija.gov.mt

2. Contact details of the national data protection authority

Office of the Information and Data Protection

Commissioner

Second Floor, Airways House

High Street, Sliema SLM 1549

Tel: +356 2328 7100

Fax: +356 2328 7198

3.19. NETHERLANDS

1. Contact details of the body to which requests for access, rectification or erasure should be addressed

Dutch National Police - Central Unit

Privacy Desk

PO Box 100

3970 AC Driebergen

The Netherlands

Tel: +31 618 144 712

e-mail: jz.le@politie.nl

2. Contact details of the national data protection authority

Dutch Data Protection Authority (Autoriteit Persoonsgegevens)

PO Box 93374

2509 AJ DEN HAAG

The Netherlands

Tel. +31-70-8888500

Fax +31-70-8888501

e-mail: info@autoriteitpersoonsgegevens.nl

website: www.autoriteitpersoonsgegevens.nl

3.20. POLAND

1. Contact details of the body to which requests for access, rectification or erasure should be addressed

National Police Headquarters
International Police Cooperation Bureau
ul. Puławska 148/150 02-624 Warsaw
Tel: +47 72 123 72
Fax: +47 72 144 94
email: bmwp.kgp@policja.gov.pl
Website: <https://policja.pl/pol/kgp/bmwp>

2. Contact details of the national data protection authority

Personal Data Protection Office
ul. Stawki 2 00-193 Warsaw
Tel: +48 22 531 03 00
email: kancelaria@uodo.gov.pl
Website: <https://uodo.gov.pl/>

3.21. PORTUGAL

1. Contact details of the body to which requests for access, rectification or erasure should be addressed

Polícia Judiciária (PJ)
Lisboa
Email: Epd-dpo@pj.pt
Website: <https://www.policiajudiciaria.pt/>

2. Contact details of the national data protection authority

Comissão Nacional de Proteção de Dados - CNPD
Av. D. Carlos I, 134-1°
1200-651 Lisboa
Tel. +351 21 392 84 00
Fax +351 21 397 68 32
email: geral@cnpd.pt
Website: <https://www.cnpd.pt/>

3.22. ROMANIA

1. Contact details of the body to which requests for rectification or erasure should be addressed

Center for International Police Cooperation

1-5 Calea 13 Septembrie, Bucharest,
5th District Romania
Tel.: +40 21 315 96 26, +40 21 314 05 40,
+40 21 314 00 25
Fax: +40 21 314 12 66, +40 21 312 36 00
email: ccpi@mai.gov.ro
Website: www.politiaromana.ro/ccpi.htm
National

2. Contact details of the national data protection authority

National Supervisory Authority for personal
data processing
B-dul Magheru 28-30 (5th floor)
1st District
010336 - BUCHAREST
Tel: +40 31 805 9211
Fax: +40 31 805 9602
email: anspdcp@dataprotection.ro
Website: <http://www.dataprotection.ro/>

3.23. SLOVAK REPUBLIC

1. Contact details of the body to which requests for access, rectification or erasure should be addressed

Ministerstvo Vnútra Slovenskej Republiky
Pribinova 2
81272 - BRATISLAVA
Fax: +421 2 5094 4397
Website: <http://www.minv.sk>

2. Contact details of the national data protection authority

Office for Personal Data Protection of the
Slovak Republic
Hraničná 12
82007 – BRATISLAVA
Tel.: + 421 2 32 31 32 14
Fax: + 421 2 32 31 32 34
email: statny.dozor@pdp.gov.sk
Website: <http://www.dataprotection.gov.sk/>

3.24. SLOVENIA

1. Contact details of the body to which requests for access, rectification or erasure should be addressed

Policija, Ministrstvo za notranje zadeve
Štefanova 2
1501 - LJUBLJANA
Tel. : +386 1 428 47 80
email: gp.policija@policija.si
Website: <https://www.policija.si>

2. Contact details of the national data protection authority

Information Commissioner of the Republic of Slovenia
Dunajska 22
1000 LJUBLJANA
Tel.: +386 1 230 97 30
email: gp.ip@ip-rs.si
Website: <https://www.ip-rs.si/>

3.25. SPAIN

1. Contact details of the body to which requests for access, rectification or erasure should be addressed

División de Cooperación Internacional,
Dirección General de la Policía,
POLICÍA NACIONAL
Avda Pío XII, 50
28016-MADRID
Tel: 9133227638
Fax: 913103620
e-mail: dcr.gabinete@policia.es

2. Contact details of the national data protection authority

Agencia Española de Protección de Datos
(AEPD)
C/Jorge Juan, 6
28001 Madrid
Tel: +34 91399 6200
Fax: +34 91455 5699
email: internacional@agpd.es
Website:

3.26. SWEDEN

1. Contact details of the body to which requests for access, rectification or erasure should be addressed

Swedish Police Authority

106 75 Stockholm

Sweden

Tel: +46 114 14

E-mail: registrator.kansli@polisen.se

Direct e-mail to Data Protection Officer:

dataskyddsombud@polisen.se

2. Contact details of the national data protection authority

IMY (Integritetsskyddsmyndigheten)

Fleminggatan 14, 7th floor

Box 8114

104 20 Stockholm

Sweden

Tel: +46 8 657 6100

E-mail: imy@imy.se

Website: <https://www.imy.se>

3.27. EDPS

European Data Protection Supervisor

Postal address: Rue Wiertz 60, B-1047 Brussels

Office address: Rue Montoyer 30, B-1000 Brussels

Tel: +32 2 283 19 00

Email: edps@edps.europa.eu

Website: edps.europa.eu

ANNEXES (TEMPLATE LETTERS)

The following template letters can be used to file your request unless the national competent authority to which you address your request asks you to use a specific standard form.

Annex 1

Template letter for requesting access

To: Title and address of the competent authority / Europol

DD-MM-XXXX,
Place

Dear Sir / Madam,

Pursuant to Article 36 of Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol), amended by Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022, and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, I _____ (name, surname), _____ (nationality), _____ (date and place of birth), _____ (address), would like to request access to my personal data processed by Europol.

Please find enclosed:

1. Copy of a valid identity document under the national law of the state (passport/identity card/driving licence (other valid identity document));
2. Copy of the legal authorisation to represent the applicant;
3. Other.

The Applicant / The Legal Representative

(Signature)

Annex 2

Template letter for requesting rectification or erasure of the data processed

To: Title and address of the competent authority / Europol

DD-MM-XXXX,
Place

Dear Sir / Madam,

Pursuant to 37 of Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol), amended by Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022, and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, I _____ (name, surname),
_____ (nationality), _____ (date and place of birth),
_____ (address), would like to request correction of factually inaccurate data relating to me or deletion of data relating to me which have been unlawfully held by Europol. My personal data should be corrected/deleted because:

Please find enclosed:

1. Copy of a valid identity document under the national law of the State (passport/identity card/driving licence (other valid identity document);
2. Copy of the legal authorisation to represent the applicant;
3. Other.

The Applicant/The Legal Representative

(Signature)

Minutes



Final

10th meeting of the Coordinated Supervision Committee (CSC)

07 September 2023, Remote

Summary

The Coordinated Supervision Committee ("the Committee") met on 07 September 2023 remotely.

Item One: Welcome and Introduction

The agenda was adopted. The members agreed to adopt the minutes and the summary of discussions of the 9th CSC meeting via written procedure.

Item Two: Borders, asylum and migration (Schengen Information System)

The European Commission (EC) presented the new Schengen Information System (SIS) and informed the members of the existing tools provided by the EC to Member States (MS) to support the SIS implementation. The CY SA informed the members of the Cyprus connection to the SIS on 25 July 2023.

The EC also presented the Schengen evaluations and informed the members that only evaluations since 02/23 fall in their entirety under the New Schengen Evaluation Framework. They also updated the members on the situation of the SCHEVAL pool of experts for 2023 and reminded them of the 2024 call. With regards to the evaluations, the EC noted that there are still separate evaluations for data protection, SIS/SIRENE and police cooperation which, however, imply some sort of coordination on the findings. A new database (KOEL) has been set up to facilitate exchange of communication among the MS and the EC.

The Committee further exchanged with the EC on the case where a person submits an access request to the SIS addressed simultaneously to several authorities and how this situation should be handled.

The CSC SEC provided an update on the number of replies received on Article 36 SIS questionnaire, and it will start drafting the report together with the rapporteurs. The Committee referred briefly to its ongoing work on the audit cycle standards.

The Coordinator reminded the members of their possibility to use the draft letter for collection of statistics on Data Subjects' Rights (DSR) adopted in the CSC June meeting, pursuant to Article 54(3) of Regulation (EU) 2018/1861 and Article 68(3) of Regulation (EU) 2018/1862.

The Committee exchanged briefly on the alerts on child abduction and members were asked for further input.

Item Three: General

The Members exchanged on the proposal to engage actively with civil society. Members agreed to limit the invitations to 3 NGOs with experience in the requested fields for the next CSC physical meeting of 29 November. The CSC SEC will send out the invitations in September.

The Coordinator reminded the members of the possibility to review the CSC RoP and asked them to brainstorm and decide whether a review is needed. There was a first exchange of views on the format of the meetings minutes to be followed. The Members agreed to have 2 deputy coordinators to prepare for the future work of the CSC, and to provide input on organisational issues in the next meeting.

Item Four: Digital single Market (IMI)

The Coordinator informed the members of the recent requests to NIMICs concerning the implementation of data protection in IMI and invited the EC to take the floor. The EC presented the IMI information sharing exercise and the updated document on national limitations. The EC invited CSC members to alert in case of similar activities and promised to share the general findings.

The rapporteurs thanked the members for their input on the recommendations on transparency obligations and agreed that an updated version will be circulated for adoption, via written procedure.

The EDPS informed the Committee about the audit to the IMI at the DG Grow premises in Brussels of the European Commission that took place in June 2023.

The next CSC meeting will be held, physically, on the 29 November 2023.

Minutes



Final

11th meeting of the Coordinated Supervision Committee (CSC)

29 November 2023, in person

Summary

The Coordinated Supervision Committee ("the Committee") met on 29 November 2023, in person.

Item One: Welcome and Introduction

The agenda was adopted. The deputy coordinator reiterated the EDPB's [plenary decision](#) of April 2023 on remote access to in person meetings. Taking into account the CSC Rules of Procedure (RoP) and the existence of exceptional circumstances in this occasion, remote access was granted to two CSC members.

Item Two: General Issues

2.1. Elections of two deputy coordinators: Sebastian Hümmeler (DE SA) was re-elected as deputy coordinator. Elections for a second deputy coordinator will take place in the next CSC meeting.

2.2. Review of the CSC Rules of Procedure (RoP): It was agreed there is no need to amend the RoP.

2.3. ETIAS Fundamental Rights Guidance Board (EFRGB): Ms. Tiina Ahtonen (FI SA) has resigned from the ETIAS Fundamental Rights Guidance Board and considering that originally three persons were appointed, it was decided at the November plenary, to proceed with two persons (one member and one alternate), without appointing an alternate to replace Ms. Ahtonen.

Item three: Police and judicial cooperation

3.1. Europol: The EDPS presented its main findings on the 2022 annual inspection report regarding Europol. The report concerned the processing of minors' personal data, targeting those under the age of 15. The EDPS also shared some findings on the 2023 annual inspection on PNR.

The EDPS further provided a state of play on the handling of several complaints against Europol, either for lack of sufficient motivation for refusing access to data subject requests or because of a late reply to data subjects' requests for access. The EDPS also updated the members on the order of the General Court in case T-578/22 that rejected its action for annulment as inadmissible.

3.2 Eurojust: Most of the EDPS recommendations were implemented. A number of issues will be addressed under the new legislative framework, as an amendment of the Eurojust Regulation is scheduled tentatively end of 2025. The next update will be provided in December.

3.3 EPPO: In April 2023, the EDPS engaged with the PT DPA and the local EPPO office in Lisbon to examine the integration of systems and the relations between the case file and EPPO's case system to raise awareness and delineate tasks and responsibilities among supervisory authorities and the EDPS.

Item four: Border, asylum and migration

4.1. Schengen Information System (SIS): The lead rapporteur presented the draft note on the legal interpretation of provisions of the audit cycle. The members discussed the starting point for the calculation of duration of the audit cycle.

4.2. AOB

4.2.1. Schengen scoreboard: Data protection has been included in the Schengen scoreboard. This will be discussed at the next CSC meeting.

4.2.2. General matters: One SA announced they are working on a follow up of the workshop on the supervision of the EU information systems to take place tentatively in January 2024 and called for ideas. A first digital technologist coffee took place on 23 November 2023.

Item five: NGOs presentation and mutual exchange

The CSC in its work programme decide to engage with civil society organisations. Two NGOs attended this kick-off session (EDRI and Access Now). The NGOs' representatives presented their projects in the fields related to the work of the CSC. The members and the two NGOs exchanged on potential synergies. The NGOs also provided valuable input to the CSC on best practices when engaging with civil society.

Minutes



Final

12th meeting of the Coordinated Supervision Committee (CSC)

19-20 March 2024, in person

Summary

The Coordinated Supervision Committee ("the Committee") met on 19 and 20 March 2024, in person.

First Day (19 March)

Item 1: Welcome and Introduction

The agenda of the first day was adopted, with the insertion of an AOB under item 2.1.

Item 2: Police and Judicial Cooperation

2.1. Europol

2.1.1 Information by the EDPS: The EDPS presented the key elements of its prior consultation Opinion on a new Facial Recognition system for Europol, which was issued on 20 December 2023 and was published on its website. There was a brief exchange among the CSC members on this new system. The CSC is to be kept informed of the developments in this regard, in particular on how the recommendations made by the EDPS will be implemented.

The EDPS also presented its opinion regarding the joint operational analysis under Article 20(2a) of the amended Europol Regulation. The EDPS explained further that it constitutes a novelty, which expresses the way Europol would like to cooperate with the law enforcement authorities of Member States. The Committee discussed the joint controllership issues that this new working method may raise between Europol and the Members States participating in the joint operational analysis, what may bring the need for enhanced coordinated supervision at central and national level, representing new challenges for the CSC.

The EDPS provided additional information on its 2023 Europol inspection, presenting first insights in relation to Europol's request of access to data in the VIS information system and to the data subject categorisation (DSC) of large data sets. The EDPS is currently finalizing its report, which shall include a set of recommendations to Europol. The CSC members discussed and acknowledged that some of the

topics addressed during the inspection (e.g. DSC of large data sets) may be important for the Committee to decide on its future activity.

2.1.2. Interpretation of lawfulness checks in the context of Article 47 ER: Under Article 47 of the Europol Regulation, the EDPS has to consult the national DPA of the MS that provided the data to Europol and has to reply within a maximum of three months. Consequently, the EDPS has to take into account the DPA's opinion when issuing its decision. There is a lengthy procedure that involves verification at Europol and at Member State level by the national DPAs, and sometimes the complexity of complaints require additional checks. It was discussed by the Committee the need to make the process more efficient, as well as the need to ensure a common understanding of the provisions and the respective obligations among the Committee's members. There was some exchange of opinions on the reading of Article 47 and the extent of the verifications at national level. It was agreed to start working on a brief guidance note for cooperation in the implementation of Article 47 complaints, containing specific steps, procedures, indicative deadlines, as well as a common understanding of the interpretation of the legal provision. A drafting team was set up for that purpose.

2.1.3 New coordinated activity on the processing of personal data in support of a criminal investigation without data subject categorization, under Article 18a of the amended Europol Regulation: It was proposed to develop a coordinated activity related to the Article 18a of the amended Europol Regulation, which provides for the possibility of Europol processing data without data subject categorisation in support of a criminal investigation of a MS. This would be in line with the CSC working programme 2022-2024, as part of addressing the big data challenge. The CSC members endorsed the activity, as it was outlined, and some CSC members volunteered as rapporteurs to start working on a checklist for inspection.

2.1.4 AOB - Point of information on last years' statistics on minors in Europol

The EDPS expressed its intention to share information with the supervisory authorities of those Member States that sent to Europol, in 2023, data on minors under fifteen years old, labelled as potential criminals or suspects. Similar information was the basis in the previous year for launching a coordinated exercise regarding minors, in which the concerned national DPAs took part. This updated information allows CSC members to carry out checks on the lawfulness of the transmission of such data, taking into account the national legal framework.

2.2. Eurojust

Some national data protection authorities have reported to the Committee that they were experiencing difficulties in supervising national judicial authorities in what regards Eurojust. Their competence is hardly recognised due to the interpretation that such data processing falls within the exception of courts when acting in their judicial capacity, provided for in Article 45 of the Law Enforcement Directive. The Committee decided to get an overview of the supervision at national level in this field, and asked all members to provide information on areas not covered by any data protection supervision, on areas supervised by a different authority, on the relevant legal provisions governing the regime, including the status of independence, in order to map such situations and decide on the way forward.

Second Day (20 March)

Item 3: Welcome and Election

3.1 Adoption of Agenda for 2nd day: The participants adopted the agenda of the second day.

3.2 Election of the 2nd Deputy Coordinator: Mr. Matej Sironič, from the Slovenian DPA, was elected unanimously as the second Deputy Coordinator of the CSC.

Item 4: General issues

4.1. Presentation on Access to Documents: The Secretariat presented the topic of Access to Documents under EU law (particularly Regulation (EU) 2001/1049), explaining the principle of transparency and the right of access to documents, its material scope, the limitations to it, the beneficiaries, the time to provide the reply and the exceptions. The members asked the Secretariat for clarifications about access to documents procedures, and the Secretariat illustrated the procedure relevant for CSC.

4.2 Takeaways of meeting with civil society: There was an exchange among the members on the takeaways as regards the participation of the civil society organisations in the previous CSC meeting as a basis for drafting a letter to those NGOs. It was also agreed to discuss in the following meetings the future dialogue with other kind of organisations of the civil society, such as academia. It was further stressed out the importance of ensuring transparency in the choice of the stakeholders with whom the CSC will engage in the future. It was also decided that the letter, after being adopted and sent, will be published in the CSC website.

Item five: Presentation of the EDPS interoperability tool and Q&A with the contractors (external academics)

The EDPS briefly introduced the tool to the members and explained the context of the study and the decision to commission it. The contractors, Dr. Teresa Quintel and Dr. Niovi Vavoula, from the University of Maastricht, joined the meeting, and presented the tool saying that it was finalized in July 2023, and that it needed constant updates due to the evolving legislative framework. The contractors illustrated how to use the tool following data flows. Based on selected scenarios, the academics showed how the tool could be used. They also advocated that there was a need for DPAs to assist individuals exercising their rights. Data subjects located outside of the Schengen area would face even higher challenges. They highlighted the complexity of the system, also quantitatively (including the keeping of logs) and strongly advised to develop a strategic approach to supervision, prioritising according to the biggest. It was suggested to follow the data flows and to have at least one expert or rather dedicated Unit for interoperability within each DPA.

Dr. Quintel and Dr. Vavoula explained that the tool presented the potential of interoperability. They ended their presentation by explaining that since the interoperability was expanding and the systems became more connected, more fundamental rights entered the discussion, for example the right to non-discrimination. This implied that more coordination between authorities would be needed, in

order not to duplicate the tasks. The CSC members congratulate the contractors for their work, followed by an exchange of views on some of the issues raised and on the possible use of the interoperability tool at national level.

Item 6: Borders, asylum and migration

6.1 EES and ETIAS: role of the CSC: The members agreed to formalize the coordination of activities in regards of ETIAS and EES in the context of CSC.

6.2 Report on ETIAS II Data Protection Workshop: The rapporteur updated the members on this workshop, underlining that a key aspect of the workshop was the discussion about which legal framework was applicable according to Article 56(2) of the ETIAS Regulation. Some guidance on this matter is of the utmost importance.

In addition to the format of the two first workshops, a series of another format, namely less formal, virtual data protection workshops will take place throughout the year. To safeguard constant representation of the CSC and to prepare the possible interventions, a small working group was created. Five SAs volunteered to be part of the working group.

6.3 Tour de table: The members were invited to share on the state of play and their involvement as regards the implementation of ETIAS at national level. Some members shared their experience at national level. The exchange revealed a very diverse picture, ranging from advanced preparations in legislation, technical equipment and procedures to delayed stages with no implementing law in place, yet. The level of involvement of the members also seemed to be diverging largely.

6.4 SIS: Article 36 questionnaire – state of play: The rapporteur provided the members with an overview of the state of play, explaining the background of the matter, the findings, the problematic areas and some considerations and recommendations, and the possible next steps. The draft report will be circulated among the members for comments and discussion.

6.5 AOB: A member raised the issue of the legal framework applicable to the SIS data processing operations and on the handling of data subjects' rights. Some members shared their approach and their experience and it was agreed to continue this exchange in a dedicated thread in the forum on Confluence.

Item 7: Digital Single Market (IMI)

The Committee adopted Recommendations on Transparency Obligations for the Internal Market Information System (IMI) to assist data controllers to be more compliant with the IMI Regulation in conjunction with the GDPR. These recommendations contain as annexes to the main text an Example of Information to be provided to data subjects (Annex 1), and a Checklist for data controllers handling the requests from data subjects when exercising their rights, in particular the right of access (Annex 2). The IMI Recommendations are to be published in the CSC website and to be conveyed by the national DPAs to the national IMI coordinators and/or national competent authorities as data controllers.

Minutes



Final

13th meeting of the Coordinated Supervision Committee (CSC)

29 May 2024, remote

Summary

The Coordinated Supervision Committee ("the Committee") met on 29 May 2024 remotely.

Item 1: Welcome and Introduction

The agenda of Part A was adopted.

The minutes of the first day of the 12th CSC meeting were adopted.

Item 2: Police and Judicial Cooperation

2.1. Eurojust

Questionnaire on data quality in the CTR: The CTR is an EU wide operational tool, which facilitates counter-terrorism investigations and prosecutions by automatically checking information for potential suspect matches and permitting collaboration between Member States through secure channels. The CSC members agreed on a questionnaire covering the data lifecycle to further investigate potential data quality issues.

2.1.3 Upcoming Audit on the Core International Crimes Evidence Database by the EDPS: The EDPS provided information on its upcoming audit on the Core International Crimes Evidence Database (CITED) on 10 & 11 June 2024 at Eurojust premises. This audit will evaluate the functioning of the system and whether it follows the EDPS' recommendations. A report is to be issued after the audit and any significant findings will be discussed in future CSC meetings.

Item 3: Agenda of Part B and Minutes

The agenda of Part B was adopted with the insertion of an AOB point under item 5.2. The minutes of the second day of the 12th CSC meeting on 20 March 2024 were adopted, except for the part concerning SIS, which the participants agreed to adopt via written procedure. The participants agreed to adopt the summary of discussions of the 12th CSC meeting via written procedure.

Item 4: General issues

4.1. Letter to EDRI and Access Now on the takeaways from the November meeting: The CSC members agreed to follow up with the NGOs participating in the November meeting by sending a letter, which will be published in the CSC website upon its sending to EDRI and Access Now.

Item 5: Borders, asylum and migration

5.1. ETIAS

5.1.1 Report of developments since the last CSC meeting: The Deputy Coordinator provided organisational information, focusing on the establishment of an “ETIAS CSC working group” in order to ensure the Committee's participation in the different ETIAS formats. The EDPS informed the Committee on the progress concerning the ETIAS implementation since the previous meeting, underlining the challenge of ensuring consistency among the controllers on the necessity of a DPIA, the concerned processing operations and the entity responsible to draft the DPIA. Discussions also touched upon the interpretation of Articles 56 and 64 of the ETIAS Regulation as well as on the issue of the allocation of responsibility for responding to data subject requests.

5.1.2 Intervention of the ETIAS Management Data Office (tbc) - State of play and data protection pending issues: The Director of ETIAS Central Unit and the Head of Data Management Office joined the meeting and informed the CSC members the timeline for the entry into operation of the ETIAS, emphasized their commitment to data protection and fundamental rights and invited the CSC members to ETIAS meetings.

They also reported that a particular data protection - working group with stakeholders aims to establish a mutual understanding of the complex legal framework and announced a new working group to support the preparation of a DPIA for the ETIAS central system.

5.1.3 Open exchange: The CSC members shared their experiences on their consultation by the controllers and the DPOs at a national level.

5.1.4 Draft letter to the Commission: During the previous CSC meeting it was proposed to send a letter to the EC to address concerns about data protection in the ETIAS system. A discussion took place on the content of the letter among the CSC members. The CSC members agreed to further work on the letter and adopt it via written procedure.

5.2. EES

5.2.1 Presentation by the European Commission (DG HOME)-on the information campaign- on the entry into operation (EiO) of the system - Q&A: As the EES system launch is expected on 6 October 2024 and the information campaign according to Article 51 of the EES Regulation is scheduled two months beforehand, during summer 2024, a discussion took place on the timeline of the national SAs' involvement. It was agreed that the CSC would contact the EC seeking clarification on the way the EC is going to comply with the obligation under Article 51 of the EES Regulation.

5.2.2 First exchange of views on Articles 53(2) and 54(2) of EES Regulation: It was discussed how the members interpreted their obligations under Articles 53(2) and 54(2) of the EES Regulation . This also touched upon the SAs' competencies under the aforementioned provisions. The CSC members concluded that this obligation falls within the general support provided by the SAs

5.2.3 Information regarding the FRA project on the EES: This project relates to fundamental rights challenges in the implementation of the EES system. FRA is going to use its findings to develop guidance for Member States and EU institutions, including pre-launch recommendations and more comprehensive practice recommendations to be implemented following the system's launch, in order to ensure the system's compliance with fundamental rights. The CSC members discussed inviting the FRA to their next meeting on 2 July 2024.

5.3. SIS

Written information by the eu-LISA DPO: The discussion of this item was postponed to a Committee's future meeting with the participation of a representative from the eu-LISA, considering that the DPO's presence and expertise are necessary for the interpretation of the specific data concerned.

5.4 AOB

5.4.1 Information by the EDPS regarding the last audit on the new SIS system launched in March 2023: The EDPS updated the CSC members on the progress of this audit at eu-LISA, underlining that its objective was the evaluation of the system's security measures, data governance practices, and the effectiveness of controls implemented prior to the system's official launch.

5.4.2 Report by the Coordinator on her participation in the Conference on ID Management in the field of migration organised by the BE Council Presidency - Written topics of the presentation: The Coordinator shared a written update on her participation in the Conference for practitioners on ID management in the field of migration organised by the BE Council Presidency.

5.4.3 Next meeting:

The next meeting of the Committee will be held, physically, on 2 and 3 July 2024.

Minutes



Final

14th meeting of the Coordinated Supervision Committee (CSC)

2-3 July 2024, Physical meeting

Summary

The Coordinated Supervision Committee ("the Committee") met on 2 and 3 July 2024, physically.

First Day (2 July)

Item 1: Internal organisation

1.1. Resignation of the Coordinator: The Deputy Coordinator announced the Coordinator's resignation and the upcoming election of the new Coordinator.

1.2. Election of a new Coordinator: Ms. Fanny Coudert, from the EDPS, was elected unanimously as new Coordinator of the CSC.

1.3. AOB: The Deputy Coordinator provided organisational information, highlighting the Committee's progress during the previous months along with the upcoming challenges due to new large-scale IT systems falling under the Committee's supervision. Discussions touched upon potential solutions, which the coordinators agreed to consider in order to improve the scheduling and the logistics of the future CSC meetings.

Item 2: Agenda of Part B and Minutes

The agenda of Part B was adopted. The minutes of Part B of the 13th CSC meeting on 29 May 2024 were adopted. The CSC members also adopted the summary of discussions for the respective part of the 13th CSC meeting.

Item 3: SIS

3.1. Presentation of the COM on Schengen evaluation mechanism

3.1.1 Schengen Scoreboard (DG HOME+DG JUST): The EC presented the Schengen Scoreboard, a key tool of the Schengen cycle, which was developed to reinforce the Schengen governance, explaining its structure, the scoring rules and the possible outcomes of the evaluation. The Scoreboard has six dimensions divided by indicators and criteria and data protection is integrated under a specific indicator. The CSC members asked for clarifications about the position of the data protection aspects and the EC clarified that all data protection aspects were included in the part Large-scale IT-systems. Questions were also raised about the criteria of assigning points and the EC provided an example in this regard.

3.1.2. KOEL platform (DG HOME+DG JUST): The EC presented the KOEL platform, which is used to upload the recommendations upon their adoption until the EC considers that the Member State has implemented all recommendations and actions, and explained the indicator on relevant recommendations in the data protection elements. The CSC members also shared their experience at national level and the EC reported that since the new Regulation entered into force one expert per area had to be nominated by the Member States and the SAs.

3.1.3. Further updates: The EC updated the Committee on the successful nominations for 2023 and stated that the call for the 2025 pool of experts was open, inviting the Member States to nominate their experts. The EC also announced that the evaluation of several countries would take place in 2025 and a thematic evaluation on the return mechanism would be conducted this year. The EC further reported on the trainings organized on data protection matters, the development of a platform to share the training material and the establishment of a Group on Harmonised Training.

The EC mentioned an upcoming workshop on integrating EES and ETIAS into the Schengen process and invited Member States to contact their national contact points in this regard. The CSC is to be kept informed in this regard, in particular on new central documents and systems.

3.2. Presentation of eu-LISA DPO on SIS statistics: The eu-LISA representative joined the meeting, presented the SIS statistics and provided a general overview of the system, of incidents and issues, data consistency check, developments and alarms and alert logs. The eu-LISA representative also presented statistics on central queries, AFIS queries, AFIS FPS and ABQ QUERIES, along with an overview of the searches and illustrated the ongoing developments, including new search functions and the interconnection between ETIAS and SIS through ESP, as well as expected developments and objectives in a longer term. The CSC members requested information about the statistics at national level and the eu-LISA representative explained why some Member States were not shown in some overviews.

3.3. Report on Article 36 alerts: Discussions touched upon the lawfulness of issuing alerts on contact persons in the SIS in cases of Article 36(2) of the SIS II Decision (now Article 36 (2) Regulation (EU) 2018/1862). Regarding the definition of contact person, the CSC members agreed that issuing alerts on contact persons on SIS is incompatible with the wording of the definition of the European provision, even if a national law authorises alerts on contact persons in national systems. This interpretation will be included in the draft report.

3.4. Checking logs of Article 12 SIS Regulations: The Deputy Coordinator shared a member's question about the methodology, the approach and the criteria to check the logs in the system. The

CSC members shared their current practices in this regard. It was suggested to set up a drafting team to frame the main issue and determine the following steps ahead of the next CSC.

3.5. AOB: A member raised a question about the SIS statistics and the issue of collecting court statistics data at national level. The Deputy Coordinators emphasized that annual reporting is not obligatory for the national SA but for the executive bodies of each Member State..

The Deputy Coordinators then provided information on the upcoming semestrial update on CSC at the following EDPB plenary meeting.

Second Day (3 July)

Item 4: ETIAS

4.1. Report of developments since the last CSC meeting: The Deputy Coordinator updated the CSC members on various workshops and working group meetings that took place. Upcoming meetings of working groups and workshops scheduled in fall 2024 were announced. Two CSC members reported on the 1st Inter - Agency meeting of the ETIAS DPIA Technical Expert Group, during which discussions took place on the data ownership concept and the definition of responsibilities and the need for support from CSC members to figure out the key issues in the DPIA of ETIAS was raised.

4.2. Letter to COM: The CSC members agreed to send a letter to the EC with Frontex Central Unit and eu-LISA in copy to address concerns and solve several criticalities concerning data protection in the ETIAS implementation system. The Committee adopted the content of the letter, and it was agreed to publish it on the CSC website.

4.3. Internal organisation: A discussion took place on the possible next steps of the coordination and the benefits of the dedicated ETIAS group, which was established during the CSC meeting on 19 & 20 March 2024 in light of the challenges for the Committee with regard to ETIAS implementation and its role in the EFRGB. The CSC members agreed to maintain the dedicated ETIAS group, and determined its commitments.

Item 5: EES

5.1. FRA project on the implementation of the EES: The FRA representative joined the meeting and provided an overview of three ongoing projects on fundamental rights implications of EU IT systems conducted by FRA. Focusing on the project on Fundamental rights implications of the EES, the FRA representative provided an overview of the methodology and the choice of countries and illustrated the fundamental rights implications of the EES, examining the fundamental rights safeguards in the system and stating the impacted rights. The CSC members were invited to participate in a discussion on the preliminary findings on 18 September 2024.

5.2. Information campaign: The Deputy Coordinator informed the CSC members that no response had been received to the letter sent to the EC. The CSC members then shared their experiences on recent developments in the information campaign at a national level.

5.3. Implementation of EES: The CSC members updated the Committee on the implementation of EES at a national level and discussions touched upon whether a DPIA would be performed in each Member State.

5.4. AOB: A member raised the issue of the right to information (Article 50) of third country nationals, on the template that has to be provided by the COM and completed by the Member States and on the material to provide.

Item 6: Agenda of Part C

The agenda of Part C was adopted.

Item 7: IMI

7.1. Management of users' access to IMI: The Deputy Coordinator reported issues of access to IMI due to the large number of users, explaining that they concerned access rights in general and potential administrative rights. It was proposed to prepare questions for discussion during the following CSC meeting and analyse the findings to figure out potential issues.

Item 8: Agenda of Part D and Minutes

The agenda of Part D was adopted. The minutes and the summary of discussions of Part A of the 13th CSC meeting on 29 May 2024 were adopted.

Item 9: Europol

9.1. Report of the EDPS: The EDPS updated the CSC members on two prior consultations regarding two tools in Europol's image and video analysis solution. One of the tools would be used for facial recognition and another tool for object identification and for scoring images, indicating the likelihood that they contain child sexual abuse material. Questions were raised about the tools functioning and the kind of cases to be investigated using these tools. The Opinions are to be sent to the CSC members upon their finalisation.

9.2. Joint activities on minors: The Deputy Coordinator shared information on the joint activities on minors, in the context of which the EDPS had requested statistics from Europol on data transfers concerning minors in 2023 and several SAs had conducted investigations. The EDPS informed the CSC members that the inspection for 2022 had been finalised, the report had been issued and a summary had been published. It was agreed to prepare a report and examine whether to standardize this activity and its format.

9.3. Complaint procedures: Internal guidance note on cooperation of supervisory authorities: During the previous CSC meeting on 19 & 20 March 2024 it was agreed to prepare a brief guidance note on Article 47 ER in order to establish a common understanding of the interpretation of the obligations and responsibilities under this provision. There was some exchange of opinions on the content of the cooperation between Europol and national authorities regarding lawfulness checks under Article 47(3) ER.

9.4. Further activities: The Deputy Coordinator raised the issue of the prioritization of Europol items, two of which remained in the list of open items, and mentioned that the possibility to use large data sets even without prior data subject categorization for investigations had not been applied. It was agreed that the items would be reviewed and potentially included in the agenda for the next CSC meeting on September 25, 2024.

9.5. AOB: The Deputy Coordinator informed the CSC members about a new proposed Regulation (COM(2023) 754 final), which involves Europol using biometric data to support Member States. Concerns were expressed about the large-scale collection of biometric data. More details on the actual implications of the new Regulation and the upcoming changes to Europol's information systems are to be found in the Annex of the legislative draft.

Item 10: Prüm II

10.1. Takeover of tasks of the CSC: The Deputy Coordinator stated that the Prüm II Regulation clearly mentions Article 62 of the EUDPR, meaning that the systems and organizations involved are subject to the Committee's supervision under Article 59(2) of the Prüm II Regulation. A discussion took place on whether the CSC members had already been consulted regarding Prüm II Regulation matters. A pilot project on EPRIS had already been carried out with the participation of several SAs.

10.2. Next steps: The CSC members discussed the following steps concerning the Prüm II Regulation and several suggestions were put forward. Clarifications were provided on the connection of Prüm II via interoperability, in particular to CIR and ESP, following the EDPS prior consultation on the structure. The CSC members agreed to set up the necessary administrative structure and point out the relevant provisions of the Regulation for the Committee's role, as well as any missing provisions from the previous legislation.

10.3. General comments

The next meeting of the Committee will be held, remotely, on 25 September 2024.

Minutes



Final

15th meeting of the Coordinated Supervision Committee (CSC)

25 September 2024, remote meeting

Summary

The Coordinated Supervision Committee ('the Committee') met on 25 September 2024, remotely.

Item 1: Agenda and Minutes

The agenda of the meeting was adopted. The minutes and the summary of the 14th meeting were adopted.

Item 2: Working methods

Discussion of new working methods to deal with the broader mandate of the CSC: discussion of proposals by members: The Coordinator informed the members of the CSC about the upcoming challenges and proposed to discuss whether the Committee needs to develop new working methods. A discussion on the number of meetings took place and the need of flexibility was highlighted by the members of the CSC. The Coordinator explained that the creation of working groups on the different bodies/systems would allow flexibility to the work of the Committee, and the members of the CSC shared their views on how they see the CSC evolving. There was a general agreement about the creation of the working groups and the organisation of the work between drafting teams and working groups. Members briefly discussed the budgeting of the CSC and it was agreed that additional systems allocated to the Committee needed to be reflected in the budget.

Item 3: Work Programme 2025-2026

Timeline for the adoption of the new Work Programme: The Coordinator launched the discussion on possible items to be added to the Work Programme 2025-2026 and added that a first draft of the Work Programme would be presented at the November meeting, in view of adopting the document in December.

State-of-Play activities under the Work Programme 2022-2024 and Activity Report: The Coordinator explained that the Activity Report that is currently being drafted covers activities until the end of 2024, in order to align the reporting activities with the Work Programme.

Priorities for 2025-2026 (calendar years) and suggestion of new items: The CSC members suggested several items for the following years, such as having more coordinated and joint inspections, working on the allocation of roles in the systems, examining and guidance on the right of access. It was also proposed to work on transversal topics relating to more than one body/system. The first draft of the Work Programme will be presented and discussed at the meeting in November.

Item 4: IMI Questionnaire: Report from drafting team

The drafting team presented the questions prepared and a discussion took place concerning the addressees of the questionnaire. A suggestion to further elaborate on the scope of the questionnaire was put forward, as well as to elaborate on the criteria of selection of the addressees. The drafting team said that the new version of the questionnaire would be discussed at the November meeting.

Item 5: EES

EES information campaign: Presentation if the EU Commission (COM): The COM presented the EES information campaign and focused on its objectives, on the messages, the visual identity, and the information materials to raise awareness among travellers. The presentation tackled the front reference to the EES website, the cases of disinformation or misinformation and the ways forward of the information campaign. The Coordinator asked for clarification on the data protection rights in the campaign, and the CSC members asked questions. With a view to the obligation of the COM to accompany the start of operation of the EES with an information campaign "*in cooperation with the supervisory authorities and the European Data Protection Supervisor*" according to Article 51 of the EES Regulation, a discussion took place on the role of the SAs in the information campaign and their involvement, the information to data subjects on the processing of their biometric data and on data subjects' rights. It was highlighted that the appropriate forum to consult the entirety of SAs is the CSC and that the Committee would welcome exchanges on the topic with the COM. It was also suggested that the members of the CSC check the state of play of the EES Information campaign at national level.

Report from FRA roundtable: One member reported to the CSC members the outcomes of the FRA Roundtable, which took place on 18 September. The particular situation of overstayers was examined in the Roundtable, and the necessity of special attention to vulnerable persons was highlighted. It was suggested that the Committee could consider the issue of overstayers and asylum seekers as part of a coordinated supervisory action.

Report from workshop: The organising SA provided information on the workshop on EES that took place on 10 September. It was agreed that the material/presentations on EES and the DTC would be shared with the members. CSC members were invited to share their information texts on EES with other members.

EES mobile apps: It was reported that there are mobile apps currently being developed and that can be used by travellers to enter their data which are transmitted via QR-code presented to the Self-Service Terminals to the national authorities' systems, for the purpose of saving time at the borders. It was suggested to invite to one of the next meetings a person from Frontex to explain the prototype that they developed.

Item 6: ETIAS

Report from ETIAS Working Group: The members reported of the discussions that took place in the second Inter-Agency meeting of the ETIAS DPIAs Technical Expert Group of 27 August. The members agreed to explore the possibility of a central IT-solution to safeguard a common secure communication channel for the information obligations under Article 64(6) of the ETIAS Regulation. The ETIAS Working Group was tasked to also consider the scope of Article 15 GDPR in their application in the framework of ETIAS. Furthermore, the Deputy Coordinator provided the CSC members with the information on the meeting of the EFRGB that took place on 3 September, and added that the next meeting would take place in mid-November. The Deputy Coordinator informed the CSC members that the first annual report of the EFRGB had been adopted, and that it would be shared. The Deputy Coordinator stated that the first meeting of the ETIAS Screening Board would take place the following week.

Item 7: SIS

Report on handling of the exercise of data subjects' rights vis-à-vis the SIS (Article 54 & 57 (4) Reg 2018/1861) - State-of-play and timeline for adoption: The Deputy Coordinator invited the CSC members to volunteer to be part of the drafting team to finalise the consolidated draft report to be sent to the COM, European Parliament and Council.

SIS audit cycle: Drafting team report of state of play: The drafting team informed the CSC members that a discussion note would be shared ahead of the next meeting to be discussed at the November meeting.

Checking logs of Article 12 SIS Regulations: Drafting team report of state of play: Following the questions to the members to share their experiences on checking logs of Article 12 SIS Regulation, a questionnaire was drafted by the drafting team on the obligations of the SAs and how to exercise them. It was agreed that the item would be discussed at the December meeting.

Report on Article 36 alerts: The drafting team had shared the draft report for comments. It was agreed that the report would be adopted via written procedure. The Deputy Coordinator thanked the members of the drafting team for the work done.

AOB: The EDPS informed the CSC members that the SIS Audit report of the EDPS will be presented at the November meeting. A suggestion from one member to invite the DPO or other qualified expert of eu-LISA to present the statistics was put forward and the Coordinator took note of it for the following meetings.

Item 8: Europol

Report of the EDPS: The EDPS presented an overview of the findings on the 2023 inspection report. Travel intelligence would continue growing in the following years. A discussion took place on the relation of the mandates of the CSC and the BTLE ESG. It was suggested to also provide the BTLE members with a presentation on the EDPS audit on PNR.

Joint activities on minors: Report from Drafting Team: According to the drafting team, the aim of the report on this joint activity was to communicate to the broader public the work of the CSC, to provide findings and recommendations and the approach to find a common approach on the inspections. The report would be structured in three sections: the description of the exercise, the general

points covered in the report and finally the annex with individual problems of national authorities in terms of actions. The drafting team invited members to exchange on their experiences.

Complaint procedure: Internal guidance note on cooperation of supervisory authorities: Report from Drafting Team: After the discussion on the item at the July meeting the work proceeded. The drafting team proposed to organise a discussion to gather a first feedback on it. It was agreed that the discussions on the guidance note would continue at drafting team level.

Item 9: Eurojust

Report from EDPS: The EDPS shared information on a prior consultation opinion on the use of a machine translation tool, and explained the purposes of the prior consultation. The prior consultation concerned the risks of producing an inaccurate output, the EDPS in the conclusions suggested to consider certain mitigation measures. It was suggested to continue the exchange on how to interpret the law on the use of AI tools by law enforcement authorities. It was agreed that the questionnaire on data quality issues related to data inserted in the Eurojust Counter Terrorism Register (CTR) will be discussed at November meeting.

Item 10: Eurojust and Europol

Secure communication channels with Eurojust and Europol: Open exchange on challenges and possible solutions for information exchange between DPAs and the agencies: The item was introduced. Communications between SAs and the agencies may contain personal data and thus, secure communication channels would be needed. According to some members, this created challenges. Following an initial exchange, it was agreed that further discussions on the topic would take place in the following meetings.

Item 11: Prüm II

For info: Planning of dedicated session with COM to present the new Prüm framework: It was agreed that at the November meeting the members of the CSC would share experiences on the implementation of Prüm II at national level and that the COM would be invited at the December meeting.

AOB

The Coordinator informed the CSC members that the dates for the meetings in 2025 had to be selected, proposed to have three meetings in person and one remote meeting and suggested the possible dates of the meeting.

The next meeting of the Committee will take place remotely on 6 November 2024.



European Data Protection Board

Anu Talus
Chair of the European Data Protection Board

Ms. Krenare Sogojeva Dërmaku
Information and Privacy Agency
Rr."Zejnel Salihu" nr.22,
10 000 Prishtinë,
Republika e Kosovës

Brussels, 9 October 2024

by e-mail only

Subject: Request to obtain the status of observer to EDPB's activities

Dear Madam,

This is in reply to your request dated 6 August 2024 asking for the status of observer to the EDPB's activities for the Kosovan Information and Privacy Agency.

The Board has taken note of the information you provided on the Information and Privacy Agency of Kosovo and on the Kosovan law on the protection of personal data.

Your request has then been evaluated by the EDPB members in the plenary meeting of 7-8 October 2024 on the basis of article 8(1) of the Rules of Procedure¹ of the EDPB.

In this regard, I am glad to inform you that the EDPB members decided to accept the request of the Kosovan Information and Privacy Agency to become an observer to EDPB's activities.

In this respect, I would kindly ask you to entrust someone in your team to contact the Secretariat of the Board (edpb-secretariat@edpb.europa.eu) for the practical arrangements.

Yours sincerely,

Anu Talus

¹ [EDPB Rules of procedure](#) - Version 8 - Adopted on 25 May 2018 - As last modified and adopted on 6 April 2022.
European Data Protection Board
Rue Wiertz, 60
1047 Brussels

Minutes



Final

16th meeting of the Coordinated Supervision Committee (CSC)

6 November 2024, remote meeting

Summary

The Coordinated Supervision Committee ('the Committee') met on 6 November 2024, remotely.

Item 1: Agenda and Minutes

The agenda of the meeting was adopted. The minutes and the summary of the 15th meeting were adopted.

Item 2: Working methods

A discussion took place on the scope of the possible mandate of so-called working groups and the decisions to be made at working group level. Several members stressed the necessity of ensuring that all CSC members are kept updated on the ongoing work within the working groups. It was agreed that the concept would be revised following the discussions that took place during the meeting, circulated for written comments and discussed during the next CSC meeting in December 2024.

Item 3: Activity report for the period 2022-2024

The Coordinator reported that the deadline to send comments would be two weeks, and that the final draft would be circulated ahead of the next CSC meeting in December 2024 in view of adoption. The Secretariat then clarified that the SIS statistics report would be removed from the Annex and adopted separately. The CSC members were invited to provide written comments to the sixth chapter of the report.

Item 4 Work Programme 2025-2026

The Coordinator introduced the topic, outlining the idea to further develop the ongoing activities included in the previous Work Programme and the suggestions made during the previous CSC meeting in September 2024, and invited the CSC members to volunteer to assume ownership of the different topics. Several members underlined the need to keep all the CSC members informed of the activities within the working groups. The Coordinator suggested implementing a mechanism to ensure this. It

was agreed to currently maintain only the EES and the ETIAS working group and continue working on the remaining topics within the drafting teams.

Item 5: IMI Questionnaire: Report from drafting team

The questionnaire had been presented during the previous CSC meeting in September 2024. Following the received comments, it had been revised, particularly regarding the addressees and its scope. The drafting team illustrated the questions. Editorial changes were made and the CSC members were invited to provide written comments.

Item 6: EUROJUST

Questionnaire on Eurojust on difficulties on supervision: The Secretariat presented the first findings following the preliminary examination of the responses received to the questionnaire. The CSC members then discussed the next steps and approach in relation to this topic. It was agreed to establish a drafting team to prepare an infonote and the CSC members were invited to participate in the drafting team.

Questionnaire on CTR: After the previous CSC meeting in September 2024 a second call for responses to the questionnaire had been circulated. Only few responses had been received in total. A new deadline to share the replies was set.

AOB: EUROPOL

Questionnaire regarding the coordinated minors action: The rapporteur recalled that a questionnaire had been circulated following the previous CSC meeting in September 2024 and invited the CSC members to send their answers to the Secretariat and the drafting team to allow the drafting team to examine the replies and discuss the approach on the first findings in the discussion group.

Item 7: SIS

SIS Statistics report: Call for volunteers: The Coordinator invited the CSC members to volunteer to join the drafting team for the SIS statistics report on handling of the exercise of data subjects' rights vis a vis the SIS (Article 54 & 57(4) Reg. 2018/1861). The SEC highlighted that a first draft of the work was shared with the CSC members.

Indirect access to SIS data: One CSC member presented a question on indirect access to SIS data, and it was agreed that the CSC members would check at national level and reply before the following meeting in December.

Item 8: EES

EES mobile app EES - presentation from Frontex: Frontex presented the EES mobile app, an app that travellers can download and that allows pre-registration of the data into EES. The CSC members asked questions on the phases of development of the app, on the different types of verifications performed by the app, on the arrangements with the service providers of the liveliness checks and the authenticity checks. The data protection aspects of the app were also examined, such as the roles of the Member

States and of Frontex, the storage period of the data in the app. Frontex specified that Member States are data controllers and that Frontex is the processor with regards to the data inserted in the app. The CSC members enquired whether Frontex can access the data inserted in the app. Questions related to the possibility for other Members States to deploy the app were asked, and Frontex explained that the app was developed as part of a research, and that if Member States decide to implement this app the travellers will have to download only one app to be able to perform the first checks to enter into different Member States.

EES WG: Letter to COM: The rapporteur provided the background to the letter, and illustrated its two key messages. A short discussion on the timeline for the implementation of EES followed, and the letter was adopted.

Item 9: ETIAS

ETIAS WG: Note on the concept of recipients in the context of DSAR: The rapporteur explained the legal question and the proposed solution discussed at working group level, and asked questions to the CSC members. A discussion on the legal analysis of the Note followed, and several CSC members intervened. It was agreed that the document would be open for comments, with a probable need to discuss the document at the following meeting. Should the CSC take a position on this question, it may be necessary to involve EDPB subgroups (BTLE, KEYP).

Representation of the CSC at the ETIAS Fundamental Rights Guidance Board - Approval of documents: It was agreed that the members of the EFRGB would share major documents in the stage of discussion with the members of the CSC, for them to be able to send comments.

- Information on the upcoming election of chair/deputy chair among the five members of the Guidance Board: The Deputy Coordinator provided information on the upcoming election of the Chair and Deputy Chair of the EFRGB, and added that the current terms would end on 14 November. The Deputy Coordinator asked whether the CSC members would agree on another candidacy as Chair. It was agreed that the Deputy Coordinator would be the candidate Chair of the EFRGB.

Report on the activities of the EFRGB - Final version of the draft guidance note on the risk for discrimination in the context of the ETIAS screening rules: A discussion took place on the approach to use when examining documents produced in the context of the EFRGB. It was agreed that the documents drafted in the context of the EFRGB would be shared in advance with the members of the ETIAS working group, and then presented as a point for information to the CSC members.

Draft guidance note on fundamental rights considerations when giving information to applicants to give effect to their right to an effective remedy and to a fair trial: The rapporteur explained that the document on the right to an effective remedy is a work in progress and that a more finalised version of the guidance note will be presented at a subsequent meeting of the CSC.

The next meeting of the Committee will take place in person on 10 and 11 December 2024.

Study on the secondary use of personal data in the context of scientific research

Final report

EDPS/2019/02-04



October 2020

This study has been prepared by Milieu under Contract No EDPS/2019/02-04 for the benefit of the EDPB.



The study has been carried out by researchers from KU Leuven (CiTiP) and University of Namur (CRIDS), with the support of researchers from Milieu and Leiden University (eLaw). The authors of the study are Teodora Lalova, Els Kindt, Eleftherios Chelioudakis, Griet Verhenneman, Antoine Delforge and Jean Herverg. National level input was provided by Carla Barbosa, Elisabetta Biasin, Gauthier Chassang, Eleftherios Chelioudakis, [REDACTED], Agnes Csonta, Antoine Delforge, Ivo Emanuilov, Danaja Fabcic, Nenad Georgiev, Dara Hallinan, Erik Kamenjasevic, [REDACTED], [REDACTED], Teodora Lalova, Zuzana Lukacova, Sjaak Nouwt, Domenico Orlando, Anastasia Siapka, Griet Verhenneman and Katerina Yordanova.

The information and views set out in this study are those of the author(s) and do not reflect the official opinion of the EDPB. The EDPB does not guarantee the accuracy of the data included in this study. Neither the EDPB nor any person acting on the EDPB's behalf may be held responsible for the use which may be made of the information contained therein.

Milieu Consulting SRL, Chaussée de Charleroi 112, B-1060 Brussels, tel.: +32 2 506 1000; e-mail: EDPB.legalstudies@milieu.be; web address: www.milieu.be.

TABLE OF CONTENT

ABSTRACT	5
EXECUTIVE SUMMARY	6
1 INTRODUCTION	8
1.1 Background and objectives of the study	8
1.2 Research questions.....	8
1.3 Methodology	9
1.4 Structure of the report	9
2 SCOPE OF ANALYSIS	11
2.1 Legal issues.....	11
2.2 Jurisdictions	11
3 INTERNATIONAL AGREEMENTS AND DOCUMENTS	12
3.1 Council of Europe: (binding) Conventions and Recommendations	12
3.1.1 Scientific research.....	12
3.1.2 Purpose limitation.....	13
3.1.3 (Secondary) use of personal data for scientific research.....	13
3.2 World Medical Association (WMA).....	14
3.3 Organisation for Economic Co-operation and Development (OECD)	15
4 LEGAL ANALYSIS OF THE NOTION 'SCIENTIFIC RESEARCH' IN THE GDPR	16
4.1 'Scientific research' in the GDPR	16
4.2 Overview and analysis of national legislation and guidance on the notion of 'scientific research'	17
5 IMPACT OF EU SECTORAL AND NATIONAL LEGISLATION ON THE PRINCIPLES OF PURPOSE LIMITATION AND LAWFULNESS IN SCIENTIFIC RESEARCH	18
5.1 Clinical Trials Regulation and the Human Tissue and Cells Directives	18
5.2 Lawfulness principle	19
5.2.1 Legal bases under Article 6(1) GDPR	19
5.2.2 Legal justifications under Article 9(2)	23
5.2.3 Difficulties in choosing a legal basis	24
5.2.4 Role of ethics committees	25
5.3 Purpose limitation and compatible use for research	26
5.3.1 Broad consent (Recital 33 GDPR).....	26
5.3.2 Overview and analysis of national legislation and guidance on broad consent.....	27
5.3.3 Primary versus secondary use of data.....	27
5.3.4 Overview and analysis of national legislation and guidance on the purpose limitation principle	30
6 LEGAL ANALYSIS OF SELECTED GDPR PROVISIONS	32
6.1 Article 11 GDPR And the obligation to inform data subjects of the reuse of data	32
6.1.1 Legal analysis of Article 11 GDPR at EU level.....	32
6.1.2 Overview and analysis of national legislation and guidance on Article 11 GDPR	33
6.2 Legal analysis of the application of the exemption to information duty for scientific research and appropriate measures under Article 14(5)(b) GDPR	34

6.2.1	Legal analysis of Article 14(5)(b) GDPR at EU level	34
6.2.2	Overview and analysis of national legislation and guidance on Article 14(5)(b) GDPR	35
6.3	Article 89(1) GDPR (obligation to de-identify data collected) and data subjects' rights under the GDPR.....	36
6.3.1	Legal analysis of Article 89(1) GDPR at EU level	36
6.3.2	Overview and analysis of national legislation and guidance on Article 89(1) GDPR	37
6.3.3	Overview and analysis of national legislation and guidance on projects using covert techniques	38
7	POLICY RECOMMENDATIONS	39
7.1	General recommendation: increased dialogue and cooperation.....	39
7.2	Specific recommendations	39
8	CONCLUSIONS	44
ANNEX 1 – FIGURES AND TABLES		45
ANNEX 2 – QUESTIONNAIRE ON RELEVANT NATIONAL LAWS AND PRACTICES.....		53
ANNEX 3 – SOURCES OF INFORMATION.....		63
ANNEX 4 - ACRONYMS AND ABBREVIATIONS		77
ANNEX 5 - ENDNOTES.....		79

ABSTRACT

The European Union (EU) has always promoted scientific research. It is increasingly a European Commission priority, particularly in the context of the current COVID-19 pandemic. Scientific research often requires the processing of personal data, including special categories of personal data (for example, in the field of medical research). To ensure that data protection law does not hinder the development of research, the General Data Protection Regulation (GDPR) provides for certain specific rules for scientific research. In particular, it facilitates the reuse of data for scientific purposes (secondary use of data). However, the term ‘scientific research’ is not defined in the GDPR and the rules concerning secondary use could be interpreted and/or implemented differently across EU Member States.

The objective of this study was to investigate the secondary use of personal data in the context of scientific research (in particular in the medical domain) by providing an overview of international agreements, EU and Member States’ legislation and practices on the principles of purpose limitation and lawfulness, and the application of data subjects’ rights in light of exemptions from the transparency obligation provided in the GDPR.

The methodology consisted of desk research (scientific literature, reports, position papers), supplemented by questionnaire responses on national laws from academic researchers with relevant expertise. In total, the study obtained input on 18 countries (out of the targeted 30 EU and European Economic Area (EEA) Member States).

The results highlighted the lack of a uniform approach among Member States on key aspects of the secondary use of personal data for scientific research. The study recommends increased dialogue between Member States’ Supervisory Authorities (SAs), sharing of national practices and interpretations, and cooperation between SAs, European institutions and bodies and key stakeholders. In addition, the European Data Protection Board (EDPB) could adopt guidelines that specifically address the secondary use of data for scientific research. The study discusses the main issues that require guidance and proposes how they might be approached.

EXECUTIVE SUMMARY

The objective of this study was to investigate the secondary use of personal data in the context of scientific research (in particular in the medical domain), by providing an overview of international agreements, European Union (EU) and Member State legislation and practices on the principles of purpose limitation and lawfulness, and the application of data subjects' rights in light of exemptions from the transparency obligation provided in the General Data Protection Regulation (GDPR).

The methodology consisted of desk research (review of scientific literature, reports, position papers), supplemented by questionnaire responses on national laws received from academic researchers with relevant expertise. In total, the study obtained input on 18 of the targeted 30 EU and European Economic Area (EEA) Member States.

The legislation analysed was not limited to the GDPR but included international agreements or documents containing data protection rules (such as Council of Europe Convention 108+) and ethical standards (such as the World Medical Association (WMA)'s Declaration of Helsinki (DH) and EU sectoral legal frameworks (e.g. on clinical trials, biobanks).

Analysis of these different legal texts and their application within the Member States examined found the following:

- Two main international frameworks apply to secondary use of personal data for scientific research: data protection rules as they have evolved historically, and ethical standards. A data controller who conducts secondary use of personal data has to consider and apply both consistently. Overlaps, including in terminology (for instance, consent as an ethical requirement versus consent as one of the possible legal bases under the GDPR) make this a challenging task. Further research on the overlap between the two frameworks would be beneficial.
- The notion of 'scientific research' is not explicitly defined in the GDPR, although some elements are provided in its Recitals. Few of the countries examined provide an overarching definition in their national legislation (with the exception of national *lex specialis*, e.g. for medical research). Based on the commonly accepted characteristics in EU and international legal texts, the **concept of scientific research** could be described or defined as: any research for a scientific purpose, financed by public authorities or the private sector, carried out in accordance with the established ethical standards and the methodology applicable in the sector concerned by the research. The scientific scope may include the development and demonstration of technologies, basic research, academic or applied research.
- On the possibility to reuse personal data for scientific research, several uncertainties remain with regard to the **lawfulness** and **purpose limitation** data protection principles, and the impact of EU sectoral laws (such as the Clinical Trials Regulation (CTR) and biobank rules) on those principles.

The choice of the possible legal basis (under Article 6 GDPR) and the most appropriate condition that could allow the processing of special categories of data (e.g. health data), pursuant to Article 9 of the GDPR for conducting scientific research, is a challenging task, particularly for transnational research. Members States often have divergent interpretations, with some still requiring consent, despite the European Data Protection Board (EDPB) and the European Commission's position on clinical trials.

The possibility to ground the secondary use of personal data in 'broad consent' (Recital 33 GDPR) is another point of divergence between Member States.

'Secondary use' is an established term in EU data protection legislation. It could pertain to either further compatible processing or non-compatible processing. There are different views at

institutional, national and scholarly level as to whether a new legal basis is required for the ‘secondary use’ of personal data. The study concluded that a legal basis is required for secondary use for scientific research purposes – this could either be the same as that for primary use or a new legal basis.

Ten of the 18 countries examined had special advice available on the implementation of the presumption of compatibility of secondary use for scientific research. The views presented varied. Finland, for example, recently established a central licensing authority to facilitate secondary processing of health and social data, which is under the custody of several controllers. Such data are now centralised at national level, with a Data Permit Authority deciding on access requests.

- The secondary use of personal data may impact the application of data subjects’ rights. A key issue here is how the rules on processing of personal data that do not require identification (Article 11 GDPR) fit with the transparency obligation and right to information of data subjects. Few Member States provide guidance on this topic, or on the related application of the exemption to information duty for scientific research in Article 14(5)(b) GDPR. In general, it is recommended that the transparency obligation be complied with via the assistance of the original data controller (through contractual agreements). France and Italy have both adopted a similar procedure, with authorisation required from the Data Protection Authority (DPA) prior to secondary use of personal data (including sensitive data), in cases where the controller (a third party) can rely on Article 14(5) GDPR. The analysis revealed no insights into Article 89(1) GDPR in the majority of the countries and there is no conclusive answer as to whether or not Member States alone can determine the appropriate safeguards, or whether the data controller can decide.

The results showed no uniform approach/interpretation among Member States on key aspects related to the secondary use of personal data for scientific research. A distinction could be made between challenges caused by a lack of uniformity in the interpretation of key elements of the GDPR and challenges caused by divergences in Member States’ implementation of the GDPR. The study thus recommends encouraging increased dialogue between Member States’ Supervisory Authorities (SAs) and information sharing on national practices and interpretations, as well as improved cooperation between SAs, European institutions and bodies and key stakeholders. The EDPB and other European institutions and bodies could establish closer exchanges in order to align their advice on the interplay of the GDPR and other sectoral laws. The EDPB could promote the set-up of relevant codes of conduct (as per Article 40 GDPR) and stress the importance of involving all key stakeholders in the creation of such codes. It could also adopt specific guidelines on the secondary use of data for scientific research. The study discusses the main issues that require guidance and proposes how they might be approached. It also emphasises the importance of empirical research to gather the views and experiences of key stakeholders, and the need to investigate the role of ethics committees in data protection matters.

1 INTRODUCTION

This chapter briefly outlines the background and objectives of the study (Section 1.1), the research questions (Section 1.2) and the methodology used (Section 1.3). The structure of this report is presented in Section 1.4.

1.1 BACKGROUND AND OBJECTIVES OF THE STUDY

This report addresses the **specific questions raised by the European Data Protection Board (EDPB)** on the topic of the secondary use of personal data in the context of scientific research. Varying legislation, practices and views exist in EU Member States with respect to the purpose limitation and lawfulness of the use of personal data for secondary research (secondary use of the data for a research purpose)¹, especially in the medical domain. The report aims to (i) explain the issues in relation to the research questions, (ii) gather Member States relevant national provisions and interpretations, (iii) find converging approaches in Member States and (iv) propose policy recommendations for the EDPB to improve harmonisation.

1.2 RESEARCH QUESTIONS

The subject of this report is the regime for the secondary use of personal data for scientific research. The study first tackles all **specific concepts** used in the General Data Protection Regulation (GDPR)². The following questions were asked by the EDPB:

- What is the meaning of ‘scientific research’ in the GDPR, in both a medical and non-medical context?
- What shall be understood by ‘primary’ and ‘secondary use’ of personal data?
- How is ‘scientific research’ understood in Member States?

The main question in this legal study concerns the meaning of the **purpose limitation and lawfulness principles** in the context of the secondary use of personal data for research in a medical and non-medical context. It seeks to provide insights into the relationship between primary use and secondary (research) use of data from the point of the overarching purpose limitation principle, compatible use and the legal grounds for secondary use for research. The following sub-questions were raised by the EDPB:

- How are these principles addressed in international agreements and documents?
- What is the impact of EU sectoral legislation, such as the Clinical Trial Regulation and Biobank Regulation on these principles?
- How are these principles addressed in legislation and guidance documentations in Member States (and EEA states)?

The research focused on the secondary use of health data in the medical context.

The third part of the study relates to limitations on **data subjects’ rights and secondary use for research**. The following areas were examined:

- The relationship between Article 11 GDPR and the obligation to inform data subjects of the secondary use of personal data (Articles 13 and 14 GDPR);
- The obligation of Article 89(1) GDPR to de-identify personal data for research and access by the controller/sponsor of clinical trials;
- The information exception for research under Article 14(5)(b) GDPR.

Finally, the research looked for **converging elements** in the national legislation of the 30 countries and formulated **policy recommendations** for the EDPB.

1.3 METHODOLOGY

The issues (stocktaking) and questions were selected by the EDPB Secretariat and sub-groups. The results of the study are mainly based on **desk research**, in particular the collection, review and legal analysis of (i) national **legislation**, relevant scientific **literature** (academic and legal practice) and reports, and (ii) the **questionnaire responses** on Member States' national laws **received from the academic researchers** in the research group and from a few selected external **national experts**.

This **questionnaire** (see Annex 2) was developed for the purposes of this study, based on the stocktake of issues mentioned above.

The **literature** selected and consulted includes not only articles in credible legal journals and recent commentaries on the GDPR, but reports and position papers published on internet platforms. The literature includes articles on the legal issues related to the use of personal data for research purposes in general and on the (re-)use of data concerning health ('health data'³) for research. While literature on the former was rather limited, literature and reports on the use of health data for research was more widely available and pointed to many open issues and diverging national interpretations. Respondents to the questionnaires also tended to focus more on the secondary use of health data.

The questionnaire was submitted to academic researchers from the research group and to several external (academic) contacts. This methodology was suitable, given the breadth and depth of international law researchers in the research team, each acquainted with the legal systems and languages of one of the 30 targeted 30 Member States and European Free Trade Association (EFTA) EEA states. This approach also avoided overburdening the national Supervisory Authorities (SAs) with requests for information.

As the research team did not include internal legal researchers for all 30 European countries, the input was limited. National law input, SA guidance (e.g. if only available in a specific language, such as Swedish, Finnish, Maltese) and insights into certain countries required **specific national language skills and legal system knowledge that was not available within the team**. The intention was to remedy this with input from selected external experts in the remaining countries. Some excellent input was received, although the confidential nature of the study mean that not all experts could be readily contacted. A further difficulty was the lack of an incentive for these external experts to invest time in researching and completing the questionnaire, which likely reduced the replies further. The responses gave rise to other issues not covered in the research questions. Finally, the study was further limited in that the inputs gathered under national law have not been validated – this is recommended to be done with SAs through interview, for example.

In total, input was gathered for 18 countries. These are not necessarily representative of the 30 EU/EEA States, however, and it is possible that some specific national positions are missing. The detailed input was structured in various tables and overviews in Excel sheets. The analysis shows general tendencies on many issues, suggesting that they could provide some insights and could usefully be examined in the remaining countries. Another approach worth further investigation (both for this and other data protection studies generally) is to review whether it is possible to cluster countries with similar traditions/views on data protection/specific data protection issues.

This report aimed to formulate recommendations based on the legal issues and findings. These recommendations are mainly addressed to the EDPB, which can investigate further consistency measures.

1.4 STRUCTURE OF THE REPORT

Chapter 2 discusses the scope of the analysis. Chapter 3 provides a brief overview of the key international agreements and documents that are useful in assessing the concepts of scientific research, the purpose limitation principle, and secondary use of data. Chapter 4 investigates the GDPR concept

of ‘scientific research’ and how it is understood in the 18 countries examined. Chapter 5 tackles the question of how to apply the purpose limitation (including compatible use) and lawfulness principles in the context of the secondary use of personal data for research. Sectoral EU legislation is briefly analysed, such as the Clinical Trial Regulation and Biobank Regulation, and the uptake and translation of these principles into national legislation and regulatory documents. The concepts of primary and secondary use are also discussed. Chapter 6 focuses on Article 11 GDPR and data subjects’ rights, including the right to information and transparency, and Article 89 GDPR. The analysis in each of the chapters comprises a short overview and analysis of relevant national legislation and guidance. Chapter 7 contains policy recommendations, with study conclusions presented in Chapter 8.

2 SCOPE OF ANALYSIS

This chapter presents the scope of the study by presenting the legal issues analysed (Section 2.1) and the national jurisdictions covered (Section 2.2).

2.1 LEGAL ISSUES

The issues analysed are described in the Terms of Reference. The most pressing questions relating to the secondary use of data for research are in the domain of ‘health data’. An important topic is **the meaning and scope of the concept of ‘scientific research’⁴**, while questions are raised about the (conditions for) **lawful grounds** for the processing of health data for secondary use.

This report discusses the **purpose specification and limitation principle** as a key principle that could or should play a role in further understanding the scope of scientific research intended by the legislator. This report does not address the use of personal data **held in public databases for scientific research⁵**. In addition, while both the report and the country inputs often mention or point to specific national regimes for **genetic data** and research, an in-depth analysis of specific characteristics, needs and harmonisation avenues of research based on or involving genetic data, while important, falls outside the scope of this study. Further dedicated and specific research on this topic is recommended. New technology and platforms play a role in the secondary use of data, chiefly by allowing more stakeholders to access and reuse data, depending on their roles of (joint) controllership. Again, this was not a focus of this study.

2.2 JURISDICTIONS

National experts provided questionnaire responses for 18 countries, of which 17 were EU and EEA countries, i.e. Belgium, Bulgaria, Croatia, Cyprus, Denmark, France, Germany, Greece, Hungary, Italy, Latvia, Netherlands, Norway, Portugal, Romania, Slovakia and Slovenia, and one former EU Member State (United Kingdom).

Of these 18 countries, 14 were covered by internal experts, i.e. researchers affiliated with the members of the consortium (KU Leuven, UNamur, Leiden University and Milieu). Three countries - France, Germany and the Netherlands - were covered by external experts known to consortium members. Denmark law was covered by internal experts, using open-access resources available in English. The study of Denmark’s legislation was thus necessarily more limited and mainly focused on the ‘Danish Data Protection Act’.

Input for the UK was received from an external expert. References to the UK are considered useful, given its influence on many of the themes of data protection in recent decades.

For some of the countries that were not covered via the input of national experts, desk research using scientific papers allowed an analysis of some of the relevant national legislation or interpretation of specific aspects⁶.

3 INTERNATIONAL AGREEMENTS AND DOCUMENTS

This chapter provides a brief overview of key international agreements and documents that are useful in assessing the concepts of scientific research, the purpose limitation principle, and secondary use of data. The roots of the purpose limitation principle can be traced to various international agreements pertaining to data protection. In addition, when investigating how the principle applies in the context of scientific research, medical research provides a useful example. Therefore, this chapter presents and discusses international documents in both the field of data protection ethical standards in health research. The latter, in particular, may be seen as encoding prevailing assumptions and acceptance of (i) the scope of medical research, (ii) compatibility with initial collection(s) and (iii) expectations of society and individuals.

Two general remarks are useful here. Firstly, consent as referred to in the majority of documents discussed below refers to consent as an ethical safeguard to participate in research, and should not be confused with consent as one of the possible lawful grounds based on Article 6(1)(a) GDPR (see Section 4.2)⁷.

Secondly, it is commonly accepted that the purpose limitation principle consists of two building blocks: ‘purpose specification’ (personal data must be collected for specified, explicit and legitimate purposes) and ‘use limitation’ (personal data must not be further processed in a manner that is incompatible with those purposes)⁸. Both concepts are embedded in Council of Europe (binding) conventions and recommendations. Also related to ‘use limitation’ is the notion of presumed compatibility of secondary use of personal data for scientific research (Article 5(1)(b) GDPR), i.e. secondary use for the purposes of scientific research shall not be considered to be incompatible with the initial purposes.

Section 3.1 discusses the conventions and recommendations adopted by the Council of Europe⁹. Sections 3.2 and 3.3 provide information about documents which have mainly an ethical character and value, i.e. those adopted by the World Medical Association (WMA) and the Organisation for Economic Development and Co-Operation (OECD).

3.1 COUNCIL OF EUROPE: (BINDING) CONVENTIONS AND RECOMMENDATIONS

3.1.1 Scientific research

Council of Europe Convention 108 and 108+

Neither Convention 108 (Convention for the protection of individuals with regard to automatic processing of personal data)¹⁰ nor 108+ (Protocol amending the Convention for the protection of individuals with regard to automatic processing of personal data)¹¹ defines the notion of scientific research. They do, however, provide special derogations to some duties incumbent on the data controller¹².

In the Explanatory Report, the Council of Europe mentions, just as the EU does in the GDPR, that the research must be compliant with ‘*the recognised ethical standards for scientific research*’¹³.

However, Convention 108+ states that the **purposes of processing the data for scientific research aims at** ‘*providing researchers with information contributing to an understanding of phenomena in varied scientific fields (epidemiology, psychology, economics, sociology, linguistics, political science, criminology, etc.) with a view to establishing permanent principles, laws of behaviour or patterns of causality which transcend all the individuals to whom they apply*’¹⁴.

Council of Europe Recommendation (97)18 concerning the protection of personal data collected and processed for statistical purposes¹⁵

Recommendation (97)18 provides a kind of definition of the concept of scientific knowledge, stating

that ‘scientific knowledge consists in establishing permanent principles, laws of behaviour or patterns of causality which transcend all the individuals to whom they apply’¹⁶.

It also states that ‘in the biological and human sciences, much of the research process involves experimentation. In this area, personalised intervention is basic on research, even though statistical analysis may come into play at a later stage. This type of research calls for specific ethical and legal rules which have no place in the field of statistics as defined here’¹⁷.

3.1.2 Purpose limitation

Council of Europe Convention 108 and 108+

Both building blocks of the purpose limitation principle were introduced in Convention 108 and retained in Convention 108+. Article 5(b) of Convention 108 included the requirement that the purpose of the data processing should be specified (purpose specification)¹⁸. Article 9 provided for the possibility of derogations from this provision under specific conditions, thus generalising the principle that data can be processed for purposes other than the original ones only under specific circumstances (use limitation). However, Convention 108 did not provide information about the conditions under which the processing of personal data for scientific research could be allowed.

3.1.3 (Secondary) use of personal data for scientific research

Council of Europe Recommendation (81)1 on medical databanks¹⁹

In 1981, the Council of Europe adopted Recommendation (81)1, which contains principles for ‘medical care, public health, management of medical care or public health services and medical research’ (Article 1(1)). As it contains specific provisions on ‘procedures for requests for use of data for purposes other than those for which they have been collected’ (Article 3(1)(k)), it complements Convention 108, which failed to specify conditions for secondary use of personal data for research. Article 5(4) seems to suggest – based on arguments *a contrario* – that it should be allowed to communicate and share information collected in medical databanks for the purposes of medical research²⁰. Article 5(5) seems to confirm this conclusion, as it allows that data on the same individual from different databanks can be linked for the purposes of medical care, public health or medical research, in accordance with the relevant regulations. However, sharing and linking information is limited, i.e. it must be covered either by a shared obligation to ‘medical secrecy’ or the ‘expressed and informed consent’ of the individual²¹.

Council of Europe Recommendations R(97)5 and CM/Rec(2019)2 on protection of health-related data²²

In 1997, Council of Europe Recommendation R(97)5, on the use of health data, mentioned secondary use for research purposes, thus providing more explicit requirements than Recommendation (81)1. It included a provision that explicitly allowed secondary use for research purposes. In additionn to **informed consent** for one or more purposes, **authorised disclosure by a designated body** for a ‘defined scientific research project concerning an important public interest’ or law providing for scientific research as ‘a necessary measure for public health reasons’²³, the **healthcare professional** (e.g. treating physician) has a unique position in that they are allowed to ‘further process’ medical data from their patients **‘to carry out their own medical research’**, ‘subject to complementary provisions determined by domestic law’, on the condition that the **data subject has been informed and was given the opportunity to opt-out (Article 12(3))**²⁴. This addition of ‘own medical research’ of healthcare professionals based on laws on the use of medical data suggests that such ‘own medical research’ of the **healthcare professional is not considered incompatible, whereby domestic law would presumably provide the legal ground and/or safeguards**. In other words, this addition could be seen as codification of reasonable expectations of society and data subjects at that time, allowing this type of research, provided it is transparent and consenting.

The distinction between medical research conducted by the treating physician and that conducted by others was initially made in 1997, raising the question of whether it remains relevant or the reasonable expectation of the patient has changed²⁵. In other words, whether data subjects should be aware of or

expect that in order to facilitate scientific progress in the interest of society, health data need to be further processed by several people with different expertise.

The issue of multidisciplinary research was reflected in the 2019 Recommendations by the Council of Europe, which replaced Recommendation (97)5²⁶. It is now indicated that not only 'healthcare professionals who are entitled to carry out their '**own medical research**', but also '**other scientists in other disciplines**' should be able to use the health related data 'which they hold' for research purposes, as long as the data subject has been informed of the possibility beforehand and appropriate safeguards are in place (e.g. explicit consent or the assessment of a competent body)(Article 15(8)).

The impact of this provision on the purpose specification and use limitation principle should be considered carefully. While it may broaden the number and type of people who may gain access to a certain dataset and, as such, affect the use limitation principle (the second building block of purpose limitation), it should not cause a shift in the requirement for purpose specification (the first building block).

Council of Europe Recommendations of 2016(6) on research on biological materials of human origin²⁷

The Recommendation states that the interests and welfare of the human being **shall prevail over the sole interest of society or science**²⁸. Obtaining and storage of biological materials for future research can be based on either consent or authorisation, prior to which the individual concerned should be provided with comprehensible information (Article 10). Biological materials can only be used in a research project if the latter is within the scope of the consent or authorisation given by the individual (Article 21(1)). For uses not in the scope of the original consent/authorisation, reasonable efforts should be made to contact the person concerned and obtain consent/authorisation (Article 22(2)(a)). If the attempt to contact the person is unsuccessful, an exception may be made where the research addresses an important scientific interest and is in accordance with the principle of accountability (Article 22(2)(b)(ii)).

3.2 WORLD MEDICAL ASSOCIATION (WMA)

Declaration of Helsinki (1964-2013-...)²⁹

The principal international document on medical research - which is also a form of self-regulation by healthcare professionals - is the Declaration of Helsinki (DH). Initially proclaimed in 1964 by the WMA, and with regular updates (most recently in 2013), it aims to set **moral and ethical medical research principles and standards**³⁰. Its principles have broad scope and are applicable in many domains, including clinical trials and the use of human material stored in biobanks³¹. It should be noted, however, that the Clinical Trials Regulation (CTR)³² refers to an older version of the DH (2008), see Recital 80 CTR. The primary purpose of medical research involving human subjects is to generate **new knowledge** - more specifically, to understand, improve and evaluate³³. However, the interest of the individual will always prevail, and participation shall be voluntary. This translates, in principle, to '**informed consent**' (Article 25 *et seq.* DH). As for the use of identifiable human material or data, such as **research on material or data in biobanks or similar repositories**, consent shall be sought, **unless if impossible or impracticable**, in which case research ethics committees will have to consider or approve their use (Article 32 DH 2013).

The **notion of medical research** has a well-developed meaning in documents such as the DH, imposing requirements on its purpose, methodology, and publicity of results (Articles 6, 35-36 DH). It is worth examining the extent to which the DH may influence other regulations. In particular, whether the conditions and understanding of the concept of medical research as presented in the DH may impact on the notion of scientific research under the GDPR.

Another key question is whether the replacement of consent by ethics committees' approval for identifiable human material has consequences, or is to have an effect under data protection³⁴.

A third and most important question in relation to data protection is whether medical research, as understood in the DH, is (i) to be considered secondary use, and thus (ii) requiring a new legal basis, which could be different from explicit consent.

Declaration of Tapei on ethical considerations regarding health databases and biobanks (2002-2016- ...)³⁵

The Declaration of Taipei (DT) is a complement to the DH³⁶. The DT is unique in that it focuses on health databases and biobanks together and thus achieves a new level of standardisation in the field³⁷. The DT provides a definition of biobanks³⁸ and supports broad consent by specifying the criteria for its validity³⁹. Some authors have criticised the DT for being too committed to individual patient consent (as opposed to a public health ethics approach)⁴⁰. Although the DT contains a waiver-of-consent provision, its scope is much more restricted than that of Article 32 of the DH. Namely, Paragraph 16 of the DT specifies that '*in the event of a clearly identified, serious and immediate threat where anonymous data will not suffice, the requirements for consent may be waived to protect the health of the population. An independent ethics committee should confirm that each exceptional case is justifiable.*' Additionally, critics noted the uncertainty as to how the DT applies to secondary research⁴¹, with Ballantyne observing that '*If the Declaration is intended to apply to this research, the ethical approach is remarkably restrictive. If the Declaration does not apply to this research, its scope of application is severely limited*'⁴².

3.3 ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD)

The 2009 OECD Guidelines for Human Biobanks and Genetic Research Databases (HBGRD Guidelines)⁴³ represent an important political commitment on the part of the member countries. Principle 4.B states that '*prior, free and informed consent*' should be obtained for each participant in a biobank/genetic research database. This consent for participation in a biobank is **not** the consent foreseen in the GDPR as a legal basis (Article 6(1)(a) GDPR). However, the biobank may also provide for '*obtaining consent/authorisation from an appropriate substitute decision-maker, or for obtaining waiver of consent from a research ethics committee or an appropriate authority, in accordance with applicable law and ethical principles pertaining to the protection of human subjects*'⁴⁴. Upcoming national legislation is likely to address this, such as the Belgian Biobank Act⁴⁵.

In conclusion, there are two main frameworks that apply to secondary use of personal data for scientific (medical) research: (i) the data protection rules as they have evolved historically; and (ii) ethical standards, such as those defined by the DH (Sections 4.1.1-4.1.3). Even if the majority of the international documents are not binding, they could be considered to have important impacts on understandings of secondary use⁴⁶. Consideration of both frameworks is important, given their intersecting nature. Firstly, 'research' has a well-developed meaning in ethical standards, such as the DH. This could be of use when seeking to define 'scientific research' under the GDPR, which lacks such definition. Secondly, in order to conduct secondary use, a data controller has to comply with the ethical requirements (e.g. consent as an ethical safeguard or authorisation from a competent body, such as an ethics committee) and the rules on purpose limitation as specified in GDPR (the roots of which can be traced to Convention 108 and 108+, and Council of Europe Recommendations 81(1) and 2019(2), for example). Overlaps, including in terminology (e.g. consent as an ethical requirement versus consent as one of the possible legal bases under GDPR) complicate this task and increase the need to consider and analyse both frameworks together. Further research on the overlaps of the two frameworks would be beneficial.

4 LEGAL ANALYSIS OF THE NOTION ‘SCIENTIFIC RESEARCH’ IN THE GDPR

Section 4.1 presents legal analysis of the notion of ‘scientific research’ within the GDPR. Section 4.2 deals with the interpretation of the concept of ‘scientific research’ by European countries. The chapter closes with a proposed description of the concept of ‘scientific research’.

4.1 ‘SCIENTIFIC RESEARCH’ IN THE GDPR

Although the EDPB asked that the negotiations occurring during the adoption of the GDPR be considered here, such documentation is not fully publicly accessible and is highly sensitive, complicating its review for this purpose⁴⁷.

Article 4 of the GDPR, on definitions, does not give any definition of the concept of scientific research. However, Recital 159 gives some elements: *‘For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. [...] Scientific research purposes should also include studies conducted in the public interest in the area of public health.[...].’* This Recital also refers to Article 179(1) of the Treaty on the Functioning of the European Union (TFEU), which, unfortunately, does not give any further elements.

Recital 33 also deals with scientific research, stating that *‘[...] 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’*, as does Recital 161, which states that *‘for the purpose of consenting to the participation in scientific research activities in clinical trials, the relevant provisions of Regulation (EU) No 536/2014 of the European Parliament and of the Council (1) should apply.’*

It follows that scientific research is a concern, in particular in the medical domain, and should be seen as encompassing the various aspects of science, without, however, specifying the persons (physical or legal) who may carry out such research. Clearly, this is not limited to academic research organisations (universities, research centres, etc.) and research carried out by private entities with a commercial scope, such as pharmaceutical companies, could be qualified as scientific, providing ethical standards are followed (see below).

The text also refers to other existing legislation, including the CTR (Recital 156 *in fine* GDPR) and national legislation and standards.

In order to qualify as scientific, the research must be compliant with the ethical standards for scientific research. This may be a start of the definition of the concept.

In 2018, the Article 29 Working Party (WP) considered that *‘the notion may not be stretched beyond its common meaning and understands that “scientific research” in this context means a research project set up in accordance with relevant sector-related methodological and ethical standards, in conformity with good practice’*⁴⁸. This is in line with the concept of compliance with ethical standards. At the same time, if the definition of scientific research makes no clear reference to objectives of (general) public interest (e.g. the European Data Protection Supervisor (EDPS) mentioned ‘the aim of growing society’s collective knowledge’ in its Preliminary Opinion on scientific research)⁴⁹, the GDPR reintegrates a ‘public interest requirement’ in different recitals and indirectly in Article 6 (on compatibility between primary and secondary use of personal data)⁵⁰.

4.2 OVERVIEW AND ANALYSIS OF NATIONAL LEGISLATION AND GUIDANCE ON THE NOTION OF 'SCIENTIFIC RESEARCH'

Based on the findings and analysis of 18 Member States in this study⁵¹, **the vast majority of the countries examined do not provide** a unique general and overarching definition of the term 'scientific research' in their national legislation. In fact, an umbrella definition of the term 'scientific research' is provided in the legal framework of only five countries: Bulgaria, France, Greece, Romania and Slovenia. The German courts have attempted to interpret the term 'scientific research' and define it in terms of the methodologies used and the goals pursued⁵².

Nevertheless, definitions exist in 10 countries for specific types of scientific research in a '*lex specialis*' context, such as legislation relating to the health sector or the medical sector: Belgium, Bulgaria, France, Greece, Italy, Latvia, the Netherlands, Portugal, Slovakia and Norway⁵³. In Bulgaria and France, there is a common definition of scientific research, which can be found in sector-specific legislation. In Portugal, research is defined with reference to the Frascati Manual of the Organisation for Cooperation and Development. Additionally, the Netherlands has a commonly accepted definition for 'scientific research' explicitly in the health sector, as provided by soft law provisions (i.e. code of conduct)⁵⁴.

Germany, Italy and Portugal provide constitutional protection to scientific research, with no definition but a broad interpretation. In Finland, scientific research is distinguished from knowledge management and from development and innovation activities, for example⁵⁵. Finally, Croatia and Cyprus appear to have neither general definitions nor sector-specific definitions for the term 'scientific research'.

In Denmark, scientific research may only be done on data mentioned in Article 9(1) GDPR if the study is 'of significant importance to society'.

Table 1 in Annex 1 presents an overview of the definition of scientific research in national legislation.

The concept of scientific research could usefully be described or defined as follows: '*Scientific research is any research for a scientific purpose, financed by public authorities or the private sector, carried out in accordance with the established ethical standards and the methodology applicable in the sector concerned by the research. The scientific scope may include the development and demonstration of technologies, basic research, academic or applied research.*'

It would have been useful to have a definition, or at least a description, of the characteristics of what the GDPR intends by the wording 'scientific research', as processing for scientific research entails specific rules on some data protection principles and data subjects' rights, as provided by Article 89, that must be analysed with Recitals 156, 157 and 159 (see Section 5).

5 IMPACT OF EU SECTORAL AND NATIONAL LEGISLATION ON THE PRINCIPLES OF PURPOSE LIMITATION AND LAWFULNESS IN SCIENTIFIC RESEARCH

Chapter 5 discusses purpose limitation, compatible use and lawfulness of personal data processing in the case of scientific research. It first addresses EU sectoral legislation, such as the frameworks applicable to clinical trials and biobanks (Section 5.1), and then examines the impact of specific frameworks (with a focus on clinical research) on the lawfulness principle, by presenting the difficulty in choosing a legal basis for (transnational) research and discussing a possible role for ethics committees in data protection matters (Section 5.2). Section 5.3 tackles purpose limitation and compatible use by delineating the concept of broad consent, followed by a discussion of the concepts of primary and secondary use of personal data and the need (or not) to use a new legal basis when processing data for secondary use.

5.1 CLINICAL TRIALS REGULATION AND THE HUMAN TISSUE AND CELLS DIRECTIVES

The CTS and the Human Tissue and Cells Directives are discussed below.

Clinical Trials Regulation (CTR)

The CTR is set to replace the Clinical Trials Directive (EC) 2001/20/EC (CTD)⁵⁶. The recitals, articles and Chapter V of the CTR contain multiple references to the need for consent. Most importantly, informed consent is needed from the subject **for participation in a clinical trial**⁵⁷. Taking into account Recital 29, if data are collected for ‘future scientific research’, such as medical, natural or social science research, **outside the clinical trial protocol by ‘universities and other research institutions’**, this shall be in accordance with data protection legislation (Article 28(2) al 2), and **consent** is required (see Recital 29)⁵⁸.

The European Commission’s ‘Questions and Answers on the interplay between the CTR and the GDPR’, and the EDPB in its Opinion 3/2019 of January 2019 on these Q&A⁵⁹ aimed to provide clarity on several key issues^{60,61}. The EDPS added to the discussion with a Preliminary Opinion on data protection and scientific research⁶².

The field of clinical research is under the close scrutiny of other bodies, in particular the national SAs (usually the Ministry of Health) and ethics committees. The authorisation and oversight of clinical trials is the responsibility of Member States and this will not change with the entry into force of the CTR. This lack of regulatory harmonisation reportedly creates challenges for pan-European research, in particular⁶³.

Biobank rules

While the EU legal framework for conducting clinical trials is moving towards harmonisation⁶⁴, this is not yet the case for biobanking⁶⁵. Beier and Lenk classify the Member States into three groups for biobank regulation⁶⁶: countries with a specific law (e.g. Belgium⁶⁷), countries with composite regulations, often accompanied by soft law (e.g. Denmark⁶⁸), and countries with no specific regulation (e.g. Bulgaria⁶⁹).

A discussion about biobanks requires consideration of the so-called **Human Tissue and Cells Directives**⁷⁰, which were adopted to reshape the regulatory landscape for storage and exchange of tissue⁷¹. The Directives put a key emphasis on informed consent for tissue **donation** but do not specify any substantive consent requirements. **Scientific research is not within their scope**, as they relate to human tissue and cells intended solely for application to humans and treatment purposes⁷². However, national laws put in place to implement the Human Tissue and Cells Directives are often applicable to research and biobanks⁷³.

Due to the considerable divergence in national approaches, biobank regulations will only be referenced

with respect to the concept of informed consent.

5.2 LAWFULNESS PRINCIPLE

Data controllers can choose between six legal bases (Article 6 GDPR) on which to base the primary use of personal data. The bases are not ranked; however, in the context of clinical trials and in relation to primary use, the EDPB and the European Commission focused on a limited number of lawful grounds under Article 6 GDPR and discussed them in conjunction with the conditions for the processing of special categories of data (Article 9 GDPR).

The EDPB distinguished between two main categories of processing activities - both of which fall under the concept of primary use in clinical trials - and recommended the use of different legal bases for every category. First, processing operations related to reliability and safety purposes, and second, processing operations purely related to research activities.

Processing activities related to reliability and safety purposes

The focus of this section will be on the legal bases recommended by the EDPB in relation to the second type of processing operations (for scientific research purposes). However, in the interest of completeness, it must be specified that the EDPB considered the processing operations related to reliability and safety purposes as falling under Article 6(1)(c) GDPR – ‘legal obligation(s) to which the controller is subject’, in conjunction with Article 9(2)(i) GDRPR – ‘processing is necessary for reasons of public interest in the area of public health’. As examples of such obligations, the EDPB has given safety reporting⁷⁴ and disclosure of clinical trial data to the national competent authorities in the course of an inspection⁷⁵. To date, there appears to be no EU or national law that provides an obligation to conduct medical research, in particular clinical trials. However, if such a law does exist or is enacted in the future, it would be valuable to consider the use of Article 6(1)(c) GDPR.

Processing purely related to research activities

- 1) Explicit consent of the data subject (Article 6(1)(a), in conjunction with Article 9(2)(a) GDPR);
- 2) A task carried out in the public interest (Article 6(1)(e), in conjunction with Article 9(2)(i) or (j) GDPR); or
- 3) The legitimate interests of the controller (Article 6(1)(f), in conjunction with Article 9(2)(i) or (j) GDPR)⁷⁶.

In its most recent guidelines issued in the context of the COVID-19 pandemic, the EDPB reaffirmed these same legal bases⁷⁷. These grounds are discussed below⁷⁸ – firstly, the legal bases under Article 6(1) GDPR, and secondly, a short discussion of some of the possible justifications under Article 9(2) GDPR.

5.2.1 Legal bases under Article 6(1) GDPR

5.2.1.1 Explicit consent

Consent for clinical trial participation and biological material donation: an ethical and legal requirement *different from data protection requirements*

As the CTR rightfully points out, the Charter of Fundamental Rights of the European Union requires that any intervention in the field of biology and medicine cannot be performed without the free and informed consent of the individual concerned⁷⁹. The consent required in Article 28(1)(c) of the CTR must be seen in this context of **human participation in a clinical trial** and not as the consent required or as providing a consent or other legal basis for the processing of personal data. The EDPB and the European Commission have agreed that the CTR requirement for informed consent for human participation must not be confused with consent as a legal basis for data processing under the GDPR^{80,81}. Indeed, there are two different levels: one linked to the protection of the integrity and self-determination of the individual, and the other to the protection of their data. A parallel can be drawn with a patient

attending their doctor: in Belgium, for example, a doctor must obtain consent from their patient before carrying out any medical act, as provided by the Law of 22 August 2002 on patient rights⁸². The doctor will process data without requesting explicit consent, but using Article 9(2)(h) of the GDPR. The Human Tissue and Cells Directives and the **consent required to donate** biological material is to some extent similar, as the **consent required is to be distinguished from any consent possibly required for data processing**.

Consent for the processing of personal data in the clinical trial context

The EDPB emphasised that, depending on the circumstances, consent may not be the most adequate legal basis⁸³. This appears to be the case in the context of primary use for clinical trials, as consent may not adequately satisfy the requirement to be '**freely given**', due to the imbalance of power between the participants and the sponsor/investigator⁸⁴. A similar difficulty arises with the possibility to withdraw consent versus the archiving obligations imposed by the CTR⁸⁵. Under EU law, it is clear that personal data will be kept and processed even after the withdrawal of consent.

Verhenneman has provided a compelling academic analysis of why the use of consent as a legal basis under GDPR should be carefully considered and may not always be the most suitable option for medical research in general⁸⁶.

Other international guidance and national laws, however, **contradict this view**.

- The Council of Europe **recently pointed to consent as the preferred legal basis** for the processing of health data⁸⁷. However, it went on to specify that '*the law may provide for the processing of health-related data for scientific research without the data subject's consent*'. While the recommendations of the Council are not legally binding, they create political pressure for the acceptance of specific standards. If the recommendation is implemented in the national laws of the Council's member states (which include all EU Member States), this could conflict with the EU's guidance on the matter. At the same time, it may be argued that this would not be in breach of EU law, given the Article 9(4) GDPR possibility for Member States to maintain or introduce **further conditions, including limitations**, with regard to the processing of data concerning health⁸⁸.
- **The reasoning shall be carefully assessed.** The report of July 2019 for the Panel for the Future of Science and Technology of the European Parliament (STOA) found the arguments of the EDPB 'illogical', in particular the idea that a study participant who consents to participate in a trial might not be able to consent to data processing due to a potential power imbalance⁸⁹. Nevertheless, if a patient can freely consent to the participate in a clinical trial, they cannot choose to participate in the trial without their personal data being processed. Participation is only possible when they also consent to data processing. In addition, there is no valuable alternative, especially in last resort cases, which is a criterion that is generally used to assess the level of freedom in consent.
- The argument against consent as a legal basis in the clinical trial field is **not necessarily valid in other types of research**. A clear distinction can be made between situations in which there is an appropriate power balance and those in which there is not. Van Veen notes that for some types of research with health data (e.g. observational studies that start with completing questionnaires), consent would, in fact, be the most appropriate legal basis⁹⁰. Consent has also been reported as the preferred legal basis for the majority of **patient preference studies**, as the data collection occurs exclusively via qualitative techniques such as semi-structured interviews⁹¹. The same remains to be seen for biological material and research, for example.
- Scholars are divided: while consent as a legal basis has long been considered the 'default' option for researchers⁹², **arguments in favour of the use of other legal bases** are steadily being put forward, taking into account recent technological developments and the realities of modern medical research, especially clinical research⁹³. At the same time, one of the most prominent voices **in support of consent** is Hallinan, who stresses that consent under GDPR is the '**concrete mechanism giving voice**' to the underlying rationale of the legislation, i.e. providing the individual with informational self-determination⁹⁴. Interestingly, representatives of the pharmaceutical industry have voiced the opposite opinion, that consent often **provides 'the illusion of self-determination and protection, while the individual may actually not always read the information provided, may not always understand this information, and may not be in a position to refuse anyway'**⁹⁵. From a **practical point of view**, there is an argument that companies engaged in cross-border research

would struggle, in practice, to switch to a legal basis other than consent⁹⁶. Finally, consent as (not the preferred) legal basis for research in the context of clinical trials, should be examined in the precise context of particular research, taking into account the nature of the data (e.g. genetic data). The power imbalance is less easily distinguished in genomic research and biobanking, except in a clinical trial (see below). According to expert in genomic research, Hallinan, consent should have primacy over other legal grounds, including the research exception (Article 9(2)(j) GDPR).

This discussion – and indeed all related arguments – should be viewed against the background of the Council of Europe recommendations⁹⁷ and binding Council of Europe conventions⁹⁸. Research is, within limits, seen as compatible with the primary use of health data in the doctor-patient relationship for therapeutic purposes, but also for own medical research, except where there is an objection (see above and Council of Europe Rec(97)5 and Rec(2019); see also Rec(81)1). The Council of Europe Convention 108+ also allows compatible use for research, provided there is a legal basis, which shall not necessarily be consent. These Council of Europe recommendations and conventions thus appear support legal bases other than consent.

Consent for biological material, genomic research and biobanking

As mentioned above, Hallinan argues that consent should have primacy over other legal grounds, including the research exception (Article 9(2)(j) GDPR). His position may have to be seen in the context of his research in the area, however.

Overview and analysis of national legislation and guidance on explicit consent

Based on the findings and analysis of the 18 countries by the researchers⁹⁹, the majority of the countries examined do not impose the use of ‘explicit consent’ in the context of scientific research via case-law, codes of conduct, SA guidelines, other binding or non-binding instruments, and/or practices at national level. Only six countries - Belgium, France, Greece, Italy, the Netherlands and Romania - have related binding /non-binding instruments in place.

Table 2 in Annex 1 presents explicit consent requirements for personal data processing in scientific research.

The majority of countries distinguish consent for human participation in clinical trials from consent under the GDPR. The majority of countries do not impose consent as the legal basis for the processing of personal data¹⁰⁰. However, there are cases where such a requirement is enshrined in law. In France¹⁰¹ and Italy¹⁰², consent is imposed for genetic research. Germany¹⁰³ is the only country which imposes consent under the GDPR in the context of clinical trials. However, it was reported that in France it is common for sponsors of clinical trials to themselves decide to use consent, even though it is not mandated by law¹⁰⁴. The researchers who provided input for Germany and Italy observed that the situation may change in light of EDPB Opinion 3/2019¹⁰⁵. In Romania, participants must agree that their personal data will be examined during inspections by the National Medicines Agency¹⁰⁶.

A recommendation for further research would be to investigate the decision-making process of stakeholders involved in international research when choosing a legal basis, including they challenges they face. The consultation initiated by the European Medicines Agency (EMA) could potentially provide answers to these questions¹⁰⁷.

5.2.1.2 A task carried out in the public interest (or official authority)

Article 6(3) GDPR requires that the basis for the processing referred to in Article 6(1)(e) shall be laid down by Union or Member State law, which shall meet an objective of public interest and be proportionate to the legitimate aim pursued¹⁰⁸. This implies that relying on Article 6(1)(e) has substantially different obligations, depending on the Member State concerned.

The task carried out should be conveyed by legal provisions¹⁰⁹. Broadly speaking, this is the general

legal basis for data processing **for public sector purposes**¹¹⁰. A specific law is not needed for each individual clinical trial¹¹¹. However, Article 6(1)(e) is not limited to processing operations of public authorities but **also extends to processing by private bodies** who have been entrusted with a task in the public interest¹¹². There is **disagreement in the literature as to whether or not commercial entities** may make use of this legal basis. According to Kramer, they may not, even if such bodies operate in the public interest¹¹³. Other authors make no such distinction¹¹⁴. It appears, however, that they may, provided that their processing fulfills a public interest and the law specifies the entities vested with such a task in the public interest.

One potential challenge with using Article 6(1)(e) GDPR as a legal basis may become apparent in the context of transnational research, as the choice of legal basis influences the application of the one-stop-shop mechanism (Article 56 et seq GDPR)¹¹⁵. The one-stop-shop is crucial for controllers who conduct cross-border processing of data, allowing them to benefit from a single point of contact¹¹⁶. However, pursuant to Recital 128 of the GDPR, **the rules on the lead supervisory authority and one-stop-shop mechanism should not apply where the processing is carried out by public authorities or private bodies in the public interest**¹¹⁷. Although recitals are not legally binding, this proposition is reaffirmed in Article 55(2) GDPR, which states that Article 56 does not apply to processing carried out by public authorities or private bodies on the basis of point (c) or (e) of Article 6(1) GDPR.

The use of the ground mentioned above should also **be viewed against the background of the Council of Europe recommendations**¹¹⁸ **and binding Council of Europe conventions**¹¹⁹, as well as other international documents adopted. Reference to this legal basis of Article 6(1)(e) GDPR in combination with Article 9(2)(i) GDPR could be seen as being in line with Council of Europe Recommendation (2019)2 on the Protection of Medical Data (see Article 15).

There remains some **doubt for commercial sponsors to use this legal basis of ‘public interest’** allowing ‘compatible’ scientific research, at least in the clinical trial context. In addition, Article 6(1)(e) GDPR may **not be the best fit for pan-European studies, depending on the specific circumstances with regard to (joint) controllership**¹²⁰. Article 6(1)(e) GDPR is a legal basis that **best suits public research institutions** operating at national level¹²¹.

5.2.1.3 Legitimate interests of the controller

This legal basis is applicable **only to private sector controllers**¹²² and where ‘legitimate interest’ refers to an interest which is **‘visibly, although not explicitly, recognised’** by Union or Member State law¹²³. Processing for research purposes is not explicitly listed under Article 6(1)(f) GDPR, but **WP29 included scientific research as a legitimate interest**¹²⁴.

In order to rely on this basis, the controller must perform a ‘**balancing test**’ in line with the principle of proportionality, and the processing is not permitted if the controller’s interests are overridden by the fundamental rights and freedoms of the data subjects. The WP29 has provided a set of criteria which can be used when performing the balancing test¹²⁵.

Of interest is part of Recital 47, which references ‘**further processing**’: *‘The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing.’* The wording implies that **secondary use of data** can be based on Article 6(1)(f) GDPR. However, Kotschy states that further processing is dealt with only under the provision of Article 6(4) GDPR (compatibility assessment)¹²⁶. The question remains, therefore, whether the reasonable expectations of the data subject would only play a role in the case of compatible processing. As far as the secondary use of personal data for scientific research is deemed not incompatible, this could apply both when Article 6(4) is applied to assess compatible processing, and for research processing for which Article 6(4) should not be applied, as scientific research is always deemed not incompatible. Recital 113 GDPR also refers to legitimate interests in the context of international data transfers, and states that *‘for scientific or historical research purposes or statistical purposes, the legitimate expectations of society for an*

*increase of knowledge should be taken into consideration*¹²⁷.

The use of the ground mentioned above should be viewed against the background of the Council of Europe recommendations¹²⁸ and binding Council of Europe conventions¹²⁹, as well as other international documents adopted.

In medical research, the core ethical principles require that the rights, safety, and well-being of the individual prevail above the interests of science and society¹³⁰ (see discussion of the role of ethics committees in the balancing test below).

The EDPB has not provided further specific guidance on the application of Article 6(1)(f) GDPR in the field of research. However, a decisive criterion for the test could be found in the EDPB guidelines in the context of video-surveillance schemes¹³¹, namely the **intensity of intervention that the processing poses for the rights and freedoms of the individual**.

In conclusion, the **reasonable expectations of the data subjects will be important** at least when relying on legitimate interests, but also for the assessment of the research ‘compatibility’¹³². Article 6(1)(f) GDPR is a legal basis that could be invoked by **private or commercial research institutions provided there remains a balance with the rights and freedoms of data subjects, which shall at all times be checked**.

5.2.2 Legal justifications under Article 9(2)

In Opinion 3/2019, the EDPB confirmed that when processing sensitive data, the legal bases under Article 6 GDPR must be applied in conjunction with the conditions under Article 9 GDPR¹³³. It recommended two of the Article 9(2) GDPR conditions: (i) or (j) (see below). However, the EDPB examples are linked to a clinical trial context only. For genomic research, for instance, there are views that Article 9(2)(g) could also be a relevant condition¹³⁴.

The national input received for this study found several national academics who nevertheless perceive Articles 6 and 9 GDPR as alternatives¹³⁵. These are seen as **cumulative requirements** in some countries (including Belgium, France¹³⁶, the Netherlands¹³⁷, Slovakia¹³⁸). No information was available for the remaining countries, either in national legislation or in academic opinion¹³⁹.

- **Article 9(2)(i) GDPR – ‘processing is necessary for reasons of public interest in the area of public health’.** Similar to the legal basis under Article 6(1)(e) GDPR, this condition relies on EU or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject. As the condition is linked to public health, the considerations about the one-stop-shop mechanism described above apply. It can be concluded that the exception is narrow and best suited for national public health authorities and non-governmental organisations (NGOs)¹⁴⁰.
- **Article 9(2)(g) GDPR – ‘processing for reasons of substantial public interest’.** Again, the condition relies on EU or Member State law but goes beyond the requirements of Articles 6(1)(e) and 9(2)(i) by imposing the condition that the public interest be ‘substantial’, creating a high threshold for satisfying this condition. However, there is no definition of ‘substantial public interest’ either in the GDPR nor in EU law more broadly¹⁴¹.
- **Article 9(2)(j) GDPR – ‘processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes’.** Recital 52 of the GDPR clarifies that this justification requires implementation in EU or national law. Under this condition, the processing must be carried out in accordance with Article 89(1) GDPR, based on EU 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 interests of the data subject. Based on the legal provision in the GDPR, Georgieva and Kuner outline several conditions for the application of this exception with respect to scientific research¹⁴². Hallinan

notes that there is no clear data protection jurisprudence establishing objective principles that clarify most of the conditions, meaning that whether or not a law fulfills the criteria should be considered on a case-by-case basis¹⁴³. Finally, Meszaros and Ho argue that a general level of public interest would be sufficient for scientific research. Significantly, they also specify that a higher level of public interest – such as ‘important’ or ‘substantial’ - could justify the secondary use of sensitive data¹⁴⁴.

In conclusion, the notion of ‘public interest’ appears to play a central role in all of the main justifications under Article 9(2) GDPR. Academics Meszaros and Ho attempted to summarise the different degrees of public interest and order them from the perceived lower to highest¹⁴⁵. They acknowledged, however, that only ‘*the implementation, application and enforcement of the GDPR will clarify the meaning*’ of the different levels of public interest. Clarification of the notion is urgently needed.

Overview and analysis of national legislation and guidance on the appropriate legal basis for scientific research

The study examined whether national laws provide for an appropriate legal ground for the processing of personal data in the context of scientific research, including for secondary use, as provided under Article 9(2)(j) GDPR. **About half of the countries have implemented Article 9(2)(j) GDPR:** Bulgaria¹⁴⁶, Denmark¹⁴⁷, France¹⁴⁸, Germany¹⁴⁹, Greece¹⁵⁰, Hungary¹⁵¹, Latvia¹⁵², Portugal¹⁵³ Romania¹⁵⁴, Slovakia¹⁵⁵, Italy¹⁵⁶ and the UK¹⁵⁷. Denmark made no mention of Article 9(2)(j) GDPR but did refer more broadly to the data mentioned in Article 9(1) GDPR¹⁵⁸. The implementing legislation in some countries (Bulgaria, Latvia) does not specify safeguards, or does so in a very general way (Germany), raising the question of whether or not the national provisions fulfil the requirements of Article 9(2)(j) GDPR and whether they can be actually be relied upon. In France, several provisions allow for the possibility to process data for scientific research, in particular Article 44(3) of the *Loi Informatique et Libertés (LIL)* - processing of personal health data justified by public interest. **Estonia** has recognised research (and official statistics) as an autonomous legal basis alternative to consent¹⁵⁹. However, a role for ethics committees is foreseen in the application of this legal ground, namely in verifying that the controller complies with the requirements established by the law. In Norway, prior approval from an ethics committee is deemed to be a necessary and adequate legal basis to process personal health data in medical and health research¹⁶⁰. In Belgium, it appears unclear if the national data protection law foresees an appropriate lawful ground for the processing of personal data in the context of scientific research and health data. In the Netherlands, processing of sensitive data is allowed for research, if necessary, provided it serves a general interest, explicit consent is impossible and sufficient guarantees are foreseen¹⁶¹.

5.2.3 Difficulties in choosing a legal basis

Each of the legal bases outlined above has different implications for the rights of data subjects, the interests of the controller, and the feasibility of carrying out international research. Some Member States still require consent as the legal basis in all cases, without taking the specific case into consideration (see national input). Other legal bases previously encouraged by the EDPB (public interest in the area of public health and scientific research purposes) require the processing to be based on EU or Member State law, which sets the ground for further differences¹⁶². Each of the available legal bases creates a different set of consequences and rights¹⁶³. Stakeholders question whether the legal basis for processing data in the scope of the same research can vary at country level¹⁶⁴, pointing out that using different legal bases in the scope of the same research makes international studies more challenging and creates inequalities between patients from different countries.

The literature proposes different solutions. Some scholars argue that a uniform standard should be adopted across the Member States regarding the appropriate legal basis for processing personal data for research purposes¹⁶⁵. Others suggest that ethics committees should guide reliance on different lawful grounds¹⁶⁶. Although an in-depth analysis of these solutions is outside the scope of this study, a critical discussion of the role of ethics committees in data protection is warranted.

5.2.4 Role of ethics committees

Reports suggest that in many EU Member States compliance with data protection legislation in the scope of health research is under the scrutiny of ethics committees, which often lack appropriate GDPR training¹⁶⁷.

Examples include:

- For primary use of data: stakeholders in the field of clinical trials report that ethics committees tend to decide which lawful ground should be used, in particular impose consent¹⁶⁸;
- For secondary use of data: Cole and Towse report that the '*variable judgments of ethics committees in considering the compatibility of research applications (to re-process data) with the original trial protocols constitute a huge barrier – the outcomes are “unpredictable”*',¹⁶⁹.

Other academics, however, advocate a stronger role for ethics committees in the field of data protection¹⁷⁰. Although the GDPR itself does not address ethics committees¹⁷¹, the CTR links the ethical review required and the assessment of compliance with data protection legislation. Pursuant to Article 4 CTR, clinical trials are subject to 'scientific and ethical review' and shall be authorised in accordance with the Regulation. The same provision specifies that the ethical review may encompass aspects addressed in both Part I and Part II of the assessment report for the authorisation of a clinical trial. The specific aspects are to be determined at national level ('as appropriate for each Member State concerned'). Part II includes assessment of compliance with Directive 95/46/EC (the Data Protection Directive, DPD), the predecessor of the GDPR (see Article 7(1)(d) CTR). This assessment can be conducted either by the competent authority or the competent ethics committee, depending on the national rules.

At national level, Estonian law¹⁷² assigns ethics committees a role in the national implementation of Article 9(2)(j) GDPR. In particular, Chapter 2, Paragraph 6(4) of the national Data Protection Act states that for scientific and historical research based on special categories of data, the ethics committee of the area concerned shall first verify compliance with the terms and conditions provided for in the law. For scientific areas with no mandated independent ethics review, responsibility to verify compliance with the requirements rests with the Estonian Data Protection Inspectorate. Italy provides another example, particularly where consent cannot be the appropriate legal ground for the processing of health data for scientific research purposes, as informing the data subjects proves impossible or entails a disproportionate effort on specific grounds, or it is likely to render impossible or seriously impair the achievement of the research purpose. In such cases, the research shall be the subject of a favourable opinion by an ethics committee¹⁷³.

It is worth exploring whether the role of ethics committees in data protection could be harmonised. Although an in-depth analysis is outside the scope of this study, several points are worth noting for consideration.

Under the GDPR, ethics committees could usefully have a role in risk assessment. A risk-based approach is firmly embedded in clinical research¹⁷⁴, just as it is in the GDPR¹⁷⁵. The clinical trial sponsor must identify, evaluate and control (i.e. reduce and mitigate) the risks posed by the research, and the rights, safety and well-being of trial participants must always prevail over the interests of science and society¹⁷⁶. The main responsibility of ethics committees is to protect potential participants in research, thus part of their independent review is identification and weighing of the risk/benefit ratio. Research **risks** are not limited to possible physical harm, but can also include psychological, social, **legal** and economic ramifications. If the risk/benefit ratio is not optimal, an ethics committee may provide a conditional decision, including suggestions for revision¹⁷⁷. The risk assessment conducted by the sponsor and by the ethics committee is not a simple exercise, but includes both quantitative and qualitative evaluation and requires proper training.

Data protection - and the GDPR in particular - have a close relationship with ethics. The application of the legislation is not merely a technical exercise but always requires judgement. Hijmans and Raab highlight that this is at the core of processing based on the legitimate interests of the controller (Article 6(1)(f) GDPR)¹⁷⁸. To rely on Article 6(1)(f) GDPR, the controller must perform a balancing test, and WP29 has provided a set of criteria. The EDPB's view (albeit in a different context) is that the most decisive criterion should be the intensity of intervention that the processing of data poses for the rights and freedoms of the individual. **With their role and experience in performing risk/benefit assessments for research, ethics committees may have the expertise to advise on achieving adequate balancing when relying on legitimate interests, assuming that the composition of these ethics committees is sufficiently balanced.** Even more importantly, the new CTR states that laypersons, in particular patients and patient organisations, should be involved in the composition of ethics committees¹⁷⁹. This provides further guarantees for the respect of data subjects' fundamental rights and interests.

If this role in the risk/benefit assessment is accepted for ethics committees, a method must be found to safeguard against inequalities between studies subject to ethical review and those that are not. Ethical standards are not harmonised at EU level, and national and local ethics committees may show substantial differences when providing input on the application of Article 6(1)(f) GDPR. Harmonisation initiatives in the field of ethical standards, although nascent, are starting to appear. Most notably, this is the aim of the European Network of Research Ethics Committees, funded and supported by the European Commission¹⁸⁰. At national level, there is a Nordic initiative addressing the development of a joint Nordic electronic information portal on ethics committees' approval¹⁸¹.

In addition to risk/benefit assessment, ethics committees could also be involved as an appropriate safeguard under Article 89 GDPR. The possibility requires further in-depth investigation, perhaps using existing national examples (Estonia, Italy).

5.3 PURPOSE LIMITATION AND COMPATIBLE USE FOR RESEARCH

The purpose limitation principle is generally accepted as the cornerstone of data protection law¹⁸². However, the text of the GDPR is not sufficiently clear on application of the principle in the context of secondary use of personal data¹⁸³. EU case-law is surprisingly limited in this respect¹⁸⁴. For the purposes of this report, this section discusses broad consent and differentiates it from the purpose limitation principle. It then delineates the notions of primary and secondary use of data, which are important in understanding whether or not a new legal ground under GDPR is needed for secondary use. Finally, the national input on the purpose limitation principle is examined, including whether or not a new lawful ground is needed for secondary use, the application of the presumption of compatibility, and the potential influence of medical secrecy on purpose limitation.

5.3.1 Broad consent (Recital 33 GDPR)

The GDPR moved towards the acceptance of broad consent (Recital 33¹⁸⁵), suggesting that the Regulation adheres to a different interpretation of the purpose specification principle in the context of informed consent, compared to situations where personal data are processed under other legal bases¹⁸⁶. Recital 33 recognises that the purpose specification principle is challenging in research, particularly in the context of Big Data and AI techniques. Verhenneman advises against using Recital 33 to justify broadening the purpose specification principle, as this is not what the text indicated. Similarly, in its Q&A on the interplay of GDPR and CTR, the European Commission specified that the requirement of specific consent applies, even though the Recital provides some degree of flexibility¹⁸⁷.

WP29 had already limited the applicability of broad consent. Firstly, by stating that '*scientific research projects can only include personal data on the basis of consent if they have a well-described purpose*'¹⁸⁸, and secondly, by endorsing the need for subsequent rolling granular consents over one ex ante broad

consent¹⁸⁹. These two points were left unchanged in the recently issued EDPB Guidelines on consent¹⁹⁰. According to Hallinan, however, interpretations of the WP29/EDPB guidance limiting the utility of broad consent could run contrary to the intent of the legislator and may even be undemocratic¹⁹¹.

5.3.2 Overview and analysis of national legislation and guidance on broad consent

The study investigated how consent as a lawful ground is understood across the countries in light of Recital 33 GDPR. The findings are divergent and it is **hard to establish a strong pattern**. Around one-third of the countries investigated show support for broad consent, although the advice seems mixed¹⁹². Both Belgium¹⁹³ and Norway¹⁹⁴ specify that broad consent cannot be given to all types of research (blanket consent), but can in the case of cancer research, for example. In Germany, Recital 33 can be relied upon under certain conditions clarified by the German *Datenschutzkonferenz* – the group consisting of the independent German Federal and State SAs¹⁹⁵. Significant concerns about upholding respect for the right to information were evident in all cases. Norwegian law stipulates that '*Participants who have given broad consent are entitled to regular information about the project*'¹⁹⁶. Similarly, in France, the Bill of bioethics law (last version amended by the Senate in February 2020¹⁹⁷ and still under parliamentary discussion) mentions the possibility to provide individuals with information about the research programme (to be understood as broadening the scope of consent for further use in research and opening the way to information about broader intelligible research fields) in order to allow reuse of biological samples for genetic research without requiring the data controller to implement individual re-contacting and reconsenting. In Portugal, broad consent can be used only if the ethical standards recognised by the scientific community are respected¹⁹⁸.

Romania seems to be the only Member State that opposes the use of broad consent, instead preferring dynamic consent. However, this conclusion is based on a single study¹⁹⁹ and more research is required to establish that position with certainty.

On distinguishing between **the use of consent as lawful ground for secondary use of data, the majority of the countries examined do not appear to have included related specifications in their national laws**. More precisely, desk research found no such distinction in Belgium, Bulgaria, Croatia, Cyprus, France, Germany, Greece, Hungary, Italy, Latvia, Portugal, Romania, Slovakia, Slovenia and Norway.

No country reported that its national law/guidance provides for a distinction between the use of consent as a lawful ground for primary use of data in light of Recital 33, and for secondary use of data.

One of the researchers looking at France²⁰⁰ observed that it could be envisaged that, where broad consent is used for basing primary processing for research, the individual be asked at the time of consent if they wish to be informed of any specific projects for which the personal data collected will be processed, in the context of the broadly specified research areas mentioned in the spirit of Recital 33, in respect of Article 14 GDPR and national laws. If the individual freely and knowingly chooses not to be informed, that consent could be considered the legal basis of further processing, which in return integrates primary processing purposes. Competent ethics committees, as well as data protection officers (DPOs) or other authorities assessing the project, will have the option to accept or reject such a practice.

By way of preliminary conclusion, one of the key issues is whether or not broad consent could stretch compatible processing for research from 'primary use' to 'secondary use', including in the clinical trial context. However, concrete binding advice is needed as to the utility of broad consent.

5.3.3 Primary versus secondary use of data

Primary use is not a common term in data protection. **The DPD**²⁰¹ used the wording 'further processing' in Article 6(1)(b) in the context of the purpose specification principle, stating that further processing 'in a way incompatible' with the defined purposes is not permitted, while also stating that '*[f]urther processing of data for historical, statistical or scientific purposes shall not be considered as*

incompatible' on the condition that national law provides safeguards (for the data subjects). **The GDPR** took over the same purpose (specification and) limitation principle with a special regime for 'research'²⁰². Use of personal data for research was added to this first category of 'further processing', and understood as processing for compatible purposes, or not considered incompatible. **Other than this compatibility assumption, neither this article nor any other provisions in the GDPR indicate additional exceptions from the application of any other principles and obligations under the GDPR, such as the transparency and information obligation and need for legal grounds**²⁰³. The compatible secondary/further processing must still comply with all other rules in the GDPR.

In 2013, the Article 29 WP launched a specific view on further processing in its 'Opinion on purpose limitation' (not endorsed by the EDPB). The WP viewed the very first processing activity as separate from all subsequent processing operations²⁰⁴. As such, only the collection of data was qualified as the initial (primary) processing, with all subsequent processing activities (including the very first activities following collection, such as data storage and use) considered 'further processing'. It is plausible that the Article 29 WP in fact merely intended to say that **any further processing activity** shall be for **the same purpose(s)** as initially specified and defined before, or at the latest at, the initial collection²⁰⁵.

The Article 29 WP also stated that further compatible processing may need a separate lawful ground²⁰⁶.

In its recent Guidelines on the on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, the EDPB seems to clarify this possible misunderstanding by explaining that health data collected for conducting a clinical trial (primary use) may be reused (secondary use) for other scientific research and this usage should be classified as 'further processing [...] (secondary use)'²⁰⁷.

Two remarks are important here. Firstly, the intention of the legislator to consider processing for 'research' as not incompatible²⁰⁸ is likely inspired by the necessity or mandated '**important objectives of general public interest (of Member States or the EU)**'²⁰⁹. In other words, it is in the interest of society and the public that 'research' can be conducted, provided there are safeguards for the data subjects²¹⁰. This general public interest will vary over time, as will the expectations of data subjects²¹¹, as to the extent to which data (health, localisation data, etc.) would also be used for research purposes. Regulation could help to determine the further processing that should be regarded as compatible²¹². Secondly, the safeguards initially envisaged, such as anonymisation, pose serious issues in some contexts. Location data, if used as single data patterns (a particular location pattern that can be used to identify the data subject) are difficult to anonymise²¹³. Human tissue or body material for further research **cannot, by default, be (fully) anonymised**, and information relating to data subjects necessarily remains. Under data protection legislation, there is additional uncertainty about the precise status of human tissue or body material, more precisely (i) as a **source** of personal information rather than (ii) **personal data itself**²¹⁴. Biobanks containing body material, tissues or cells also have an unclear status. This type of information – which is now very valuable to both private and public funded research - also contains genetic information²¹⁵ on which a lot of research is based. Advances in knowledge could potentially be in the interest of the data subject or even those to whom they are genetically linked. The transfer of health data (blood samples, other body material) to biobanks, which **cannot be fully anonymised or only with difficulty, but which contain genetic information** must be taken into account in the context of analysis of compatible use, purpose and lawful grounds for research in the health sector. This is, however, not at the core of this study.

The need for a separate lawful ground for 'further processing', in particular for research, is strongly debated and questioned. Policy documents and academic papers frequently diverge on this point, even within the same country²¹⁶.

Several EU institutions appear to be in favour of a new legal basis. In its Preliminary opinion on scientific research of January 2020, the EDPS stated that a new legal basis is needed²¹⁷. The European Commission also found that the new ground '*may or may not differ from the legal basis of primary use*'²¹⁸, meaning that a new legal basis is required for secondary use. The EDPB found that the logic of the

Commission excludes the applicability of the presumption of compatibility and stated that '*the controller could be able [...] to further process the data without the need for a new legal basis*'²¹⁹. However, other EU bodies do not seem to share the same view. A recent EMA discussion paper noted that '*no legal basis separate from which allowed the collection of the personal data is required*'²²⁰. Stakeholders in the field hold a particular middle ground; for instance, the European Organisation for Research and Treatment of Cancer (EORTC) understands Recital 50 as a '*possibility to continue with the same legal basis, not an obligation*' and believes that secondary use may rely on a different legal basis²²¹. As for authoritative GDPR commentaries, some state that '*only compatible further use does not require an additional legal basis*'²²², while others conclude that the part of Recital 50 stating that no new legal basis is needed is an '*editorial mistake*' and that a new legal basis is always required²²³.

There are arguments **against the need for a (separate) legal basis**, even if they are not entirely convincing. One argument is text-based: the fact that the compatibility test of the WP of 2013 (which has now become part of the GDPR in Article 6(4) GDPR) is mentioned in Article 6 stating the grounds for lawful processing, deducing that such a test, if positive, would mean that the further processing would not require a separate legal ground. However, this cannot be deduced merely from the position of Article 6(4) – which is based on the earlier Opinion of the WP – and as this Article only discusses purpose compatibility²²⁴. Others refer to the (non-binding) Recital 50 GDPR, but understand this in different ways.

These diverging views are presented in **Table 3 in Annex 1**.

In addition to the arguments above, the study concludes that (presumed compatible) further processing for scientific research needs a legal basis²²⁵ because:

- the history of data protection legislation - the requirement of lawful processing and the need for a legal basis or ground has always been a central requirement and cornerstone, whereby data protection requirements for scientific research have not and should not be treated fundamentally differently, other than for the compatibility assumption;
- other longstanding principles should not be overturned without a clear legislative text confirming such intention (text argument);
- the meaning and wording of Article 8 of the EU Charter on Fundamental Rights²²⁶.

Notwithstanding several diverging views, a legal basis remains required²²⁷, including where data are further processed for research purposes. For presumed compatible research purposes, this could be the same or a new legal basis. If the data controller further processes (reuse) personal data, it can typically reuse the same legal basis as for the primary processing if this secondary processing is compatible. If it is not, they should – generally - obtain new consent from the data subject. Secondary processing by a different controller is more complicated when it comes to reusing the same legal basis.

The concept of further processing or further use has been used to mean different things over the years, creating confusion.

It seems clear that the term 'secondary use' is not an established term used in the EU general data protection legislation. The term is rather recent and increasingly used, in particular in national legislation²²⁸.

Secondary use could coincide with further use referring compatible processing²²⁹ or further use in the sense of use **other than** the initial processing, and non-compatible, in which case this is a 'new' or 'second' use, or also 'second(ary) use' in the strict sense²³⁰. Secondary use in the strict sense will always require a new legal ground.

An understanding of the need for a legal ground in relation to further processing/secondary use is presented in Figure 1 in Annex 1.

5.3.4 Overview and analysis of national legislation and guidance on the purpose limitation principle

Is a new legal basis required for secondary use of data?

In the **majority of countries (12 out of 18)**, this is not discussed in any way²³¹. Recently, however, Germany has suggested an innovative possibility, that the original legal basis is still valid as the basis for secondary processing²³².

Three countries require no legal basis²³³ but each of the national legal frameworks comes with a caveat. For instance, in Greece, the data protection law creates ‘a national legal basis for secondary use’²³⁴. In Belgium, academics believe that a new legal basis is not required when using data further for the purposes of academic medical research. The assessment of lawfulness is thus generally limited to an assessment of the lawfulness of the primary data collection and the appropriateness of the security measures implemented²³⁵. In Italy, secondary use of sensitive data for scientific research is subject to particularly strict requirements²³⁶. Although no new legal basis is required, third parties processing sensitive data for secondary use are obliged to obtain prior authorisation from the Italian SA²³⁷. Such authorisation may be either via an ad hoc decision, or through a general provision specifying the conditions and necessary measures that the controller has to implement (such a general provisions has not yet been implemented²³⁸). Where it is the same controller that processes the data further (i.e. originally collected for clinical activity), there is no need for authorisation. However, the Italian law imposes further conditions on the controller, such as implementing additional safeguards, obtaining ethics committee approval, and consulting the SA prior to the processing²³⁹.

The **only country in which a new legal basis appears to be required is the UK**. However, the advice of the Information Commissioner’s Office (ICO) is quite unclear²⁴⁰. Some medical research documents seem to suggest the need for a new lawful basis, but there is no definitive advice²⁴¹.

Implementation of the presumption of compatibility

Special advice is available in the majority of the countries (10 out of 18)²⁴². With respect to specific legislation, the Hungarian example is interesting, where a government committee was established (by law) to oversee the presumption of compatibility²⁴³. In France, the presumption of compatibility is seen as a ‘philosophical’ approach to scientific research and is used for establishing simplified procedures for research that serves the public interest and is bound by research ethics and deontology of health professions²⁴⁴. The Romanian Law on healthcare reform imposes a unique restriction on the processing of pseudonymised data from electronic health records for scientific research purposes, as it allows it only after the death of the person²⁴⁵. An interesting similarity can be observed between the Belgian and Bulgarian academic views; in both countries, academics emphasise the appropriate safeguards when the presumption of compatibility for scientific research applies. In Belgium, Verhenneman has observed that the compatibility test must be conducted but is limited to an assessment of the appropriate safeguards²⁴⁶, whereas in Bulgaria, the view is that the test should not be conducted at all in cases when the presumption of compatibility applies, on the condition that the controller provides appropriate safeguards²⁴⁷. The result appears to be the same, but the phrasing is fundamentally different.

In five of the countries studied, the existing advice does not go beyond the GDPR²⁴⁸. However, Italian scholars, in particular, are puzzled by the lack of conceptual clarity²⁴⁹.

Recent legislation in **Finland is noteworthy**. A central licensing authority for secondary data use²⁵⁰ has been established²⁵¹ to facilitate more efficient data use, in particular secondary processing of health data and social data under the custody of several controllers and usually requiring several authorisations from controllers for further use for research purposes. Such data are now pooled and centralised at national level at FinData²⁵². A central one-stop-shop, the Data Permit Authority, will decide on requests for access to (i) data from different controllers, (ii) national information system services ('client data in healthcare and social welfare') and (iii) registers of one or more private organisers of healthcare

services (Section 11 of the Act on the secondary use of health and social data) within specific timeframes. Secondary use of the data will be allowed for permitted purposes as defined in the law, with a revocable **licence** issued for a fixed term. The agency will collect, combine and, if necessary, pseudonymise or anonymise the data or generate the aggregated statistics requested (Section 14)²⁵³. The Act on the secondary use of health and social data provides for a clarified legal basis for data collection by the Finnish National Institute for Health and Welfare and national monitoring, and **knowledge management**²⁵⁴ by social and healthcare service providers but also for businesses to support decisions, by combining technical and commercial data with social and healthcare data. A licence may also be required for **education, information management and development and innovation** activities (Section 37)²⁵⁵, provided that the **explicit consent** of data subjects for secondary use is sought for the latter, as no category under Article 9(2) GDPR fit. Such consent is granular for each use (for processing by FinData, and by each secondary user) and is controllable for the data subject by a digital ecosystem, facilitating communication with the Data Permit Authority, including consent modification and withdrawal.

None of the 18 countries²⁵⁶ examined appear to have defined national rules on the application of the presumption of compatibility at national level in conjunction with the principle of lawfulness established under Articles 6 and 9 of the GDPR, in light of Recital 50 and Article 6(4) GDPR.

Does medical confidentiality influence the purpose limitation principle?

At international level, the WMA's Code of Medical Ethics states that a physician shall '*respect a patient's right to confidentiality. It is ethical to disclose confidential information when the patient consents to it or when there is a real and imminent threat of harm to the patient or to others and this threat can be only removed by a breach of confidentiality*'²⁵⁷. Council of Europe Recommendation (81)1 on medical databanks states that medical records may not be shared '*outside of the fields of medical care, public health or medical research*' **without** express and informed consent, **unless**, however, permitted by rules of medical professional secrecy²⁵⁸. In other words, medical research can be broadened where medical professional secrecy rules allow such communication because the receiving party is also bound by such medical secrecy. At national level, various regulations are usually applicable to medical confidentiality, including criminal codes, patients' rights laws, laws on the exercise of the medical profession, and national codes of ethics. As all health professionals understand the need for confidentiality, it can be seen as an additional safeguard when it comes to data protection.

In the majority of countries (11 out of 18) investigated for this study, no discussion on the influence of medical confidentiality on the purpose limitation principle was evident. Experts from seven countries (Belgium, Bulgaria, France, Germany, Italy, the Netherlands, and Portugal) shared their observations (see Table 4 in Annex 1), which together suggested that medical secrecy has a practical impact on the purpose limitation principle as applied in the context of scientific research (particularly in Bulgaria, France, and Italy).

It is important to note that in the context of the COVID-19 pandemic, the UK permitted general practitioners (GPs) and organisations providing health services to disseminate confidential patient data to other persons or organisations, as long as this was required for a COVID-19 purpose, e.g., preventing the spread of the virus or research²⁵⁹.

Interim conclusion:

On the ground of legitimate interest, the study concludes that specific legal grounds other than consent could be invoked, insofar as **specific conditions are met for the compatible research. As it is likely that not all research outside earlier defined projects (e.g. clinical trial) may meet these conditions, including the expectations of individuals and society, it would be useful to have a debate on the preferred ground (if such preference is to be established). Agreement by the data subject (consent) would be suitable in some cases, but not feasible in others.**

6 LEGAL ANALYSIS OF SELECTED GDPR PROVISIONS

This chapter first addresses Article 11 of the GDPR (Section 6.1), followed by Article 14(5)(b) of the GDPR, concerning the exemption from the information obligation for scientific research (Section 6.2). It also addresses the application of Article 89(1) of the GDPR, in particular the obligation to de-identify personal data, and the data subject's rights under the GDPR which may give the data controller the possibility to identify study participants (Section 6.3).

6.1 ARTICLE 11 GDPR AND THE OBLIGATION TO INFORM DATA SUBJECTS OF THE REUSE OF DATA

6.1.1 Legal analysis of Article 11 GDPR at EU level

As Article 11 GDPR has no equivalent in the DPD²⁶⁰, there is no relevant case-law as yet. Surprisingly, Article 11 has not been subject to much academic discussion²⁶¹, although it has sparked debate within research community from time to time. Prior to the GDPR, researchers argued that identifying information was sometimes maintained in order to meet data subjects' requests, e.g. for correction or removal²⁶².

Some issues persist with the new Article 11 GDPR. In literature, it remains unclear whether Article 11 is about anonymous or pseudonymous data. As anonymous data is out of the scope of the GDPR, the study has taken it to relate solely to pseudonymous data²⁶³, the understanding of which appears to be generally accepted in literature, particularly in authoritative GDPR commentaries²⁶⁴. Another issue is Article 11's classification and legal impact²⁶⁵. In the context of clinical research, 'reasonable measures to verify the identity of a data subject' (Article 11(2) GDPR and also Recital 64) may be difficult to define. As established by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use (ICH) Guideline for Good Clinical Practice (GCP), the sponsor receives only coded (i.e. pseudonymised) data concerning the trial subjects (Principles 1.58 and 5.5.5), while the key for identification is held by the investigator. Patients receive all relevant information (about the trial and data protection notices) via the investigator and are not contacted directly by the sponsor. In that respect, if a patient provides their name, or even their ID, directly to the sponsor, the information may not be sufficient to identify the data subject (as the sponsor does not have the key code, nor the right to obtain it from the investigator, pursuant to GCP)²⁶⁶. Finally, there is a question as to whether accepting such additional information is a separate processing activity. The GDPR commentary²⁶⁷ attempts to answer this question. In particular, Georgieva is of the opinion that the additional information required under Article 11(2) cannot be interpreted as a legal basis for data processing pursuant to Article 6(1), and the controller is still required to undertake the purpose compatibility test pursuant to Article 6(4) GDPR²⁶⁸. The controller must clarify which 'additional information' is needed. Another interpretation could be that such processing is necessary to comply with the controller's legal obligation set forth in Article 11(2) GDPR, thus the legal basis for the processing would be Article 6(1)(c) GDPR – 'legal obligation to which the controller is subject'.

The major issue, however, is how Article 11 GDPR fits with the transparency obligation and right to information of data subjects, particularly Article 14(5)(b) GDPR. Compatibility with the fundamental right to data protection as set out in Article 8 of the EU Charter on Fundamental Rights must also be assessed²⁶⁹.

It is useful here to draw a distinction between different scenarios common in research, and different kinds of research:

- Where a data controller itself reuses data and (anonymises or) pseudonymises that data itself, Article 11 GDPR does not prevent that data controller from informing the data subject prior to the reuse of data. On the contrary, if a **data controller reuses data but obtained such (anonymised or) pseudonymised data from another party**, Article 11 could prevent information being given to

the data subject prior to the reuse of data. This could deprive the data subject of their fundamental right to fairness of data processing. A potential solution could be that the original data controller provides the information to the data subject (see Section 6.1.2 for an interesting suggestion from Belgium).

- The above risk to fairness could be argued to be more likely in specific research contexts, which shall be determined. For example, research on pseudonymised personal data for the development of an IT tool is likely to impact data subjects less than research on pseudonymised health or genetic data. In the latter case, the risks are far greater in case of a data breach. **In these cases, the transparency obligation can for these purposes (to be determined) be complied with via the assistance of the original data controller through contractual agreements²⁷⁰.**

This is especially relevant in clinical trials, where an agreement between the investigator and the sponsor could foresee such an information obligation. From the point of view of a sponsor, relying on Article 11 GDPR is possible for patients who have been lost to follow-up, e.g. where the chain to the investigator is broken (see Table 5).

Table 5: Relying on Article 11 GDPR in clinical trials

Primary data collection	Retrospective research²⁷¹
<ul style="list-style-type: none"> ▪ if patient is lost to follow-up²⁷² (as the link with the investigator is broken) 	<ul style="list-style-type: none"> ▪ after the end of the mandatory follow-up period after the end of the clinical trial

However, even when the sponsor can rely on Article 11 GDPR, a good practice may be to contact the investigator and inform them that further research is being conducted, in case the investigator later gets in touch with the patient.

6.1.2 Overview and analysis of national legislation and guidance on Article 11 GDPR

In the majority of European Member States, no specific information was available on Article 11 GDPR²⁷³. For Germany, one academic assumed that there is little guidance specifying the details of information obligations in research because the obligations seem conceptually and practically clear to the research community (where the idea of fairly and transparently providing information to research subjects has a long history in research ethics)²⁷⁴. In Italy, the SA generally agrees that information should always be pursued when possible but where this is not possible, information obligations should be simplified²⁷⁵. In the UK, little guidance is available, with the exception of the Health Research Authority Guidance, which suggests that '*[w]hen personal data obtained from other sources is subject to a research exemption, the data controller must make the transparency information publicly available*', which does not contradict the GDPR²⁷⁶.

Academic opinion was available for three countries. **In Bulgaria**, Article 11 GDPR was specifically discussed in a GDPR commentary. The authors outlined the distinction between the processing of anonymous data (Recital 26 GDPR) and the processing of data which do not, or no longer, require the identification of the data subject by the controller (Article 11 GDPR). In the latter case, the data controller is processing data of identified or identifiable subjects but has to assess the necessity of collecting or storing identifying information. This means that Article 11 refers to two types of situations²⁷⁷:

- **Where the controller is processing personal data, but not all of the processing activities require the identification of the data.** In relation to the transparency obligation, the authors write: '*[...] no derogations from the right to information are inscribed neither in Art. 11, nor in Art. 12, [therefore] the data controller has to guarantee the transparency of processing in all cases. When data are collected from the data subject, he has to be informed about the identity and contact details of the data controller, the contact details of the data protection officer, the purposes of the processing and the legal basis, the recipients and categories of recipients, the period for which the personal data will be stored, and other relevant details, as listed in Art. 13 of the GDPR*'.
- **Cases where personal data are already collected but identification of the data subject is no longer required.** Pursuant to the second hypothesis presented in Article 11(1) GDPR, during the

first stage of processing, the data controller collects data of identifiable natural persons. However, in the course of the processing it is discovered that identifying the data subjects is no longer needed. The authors provide the following examples: '*it may be that the primary purposes for which the data were collected, have changed*'; '*it is possible that the storage periods have expired* and that, *in order to comply with the storage limitation principle, the data controller would not be able to store the data any longer in a form that would allow the identification of the data subjects*'. With respect to the second example, Toshkova-Nikolva and Feti explain that storing data for longer periods (than originally planned) is possible only as long as they will be processed solely for archiving purposes in the public interest, scientific and historical research purposes or statistical purposes, and when applying technical and organisational measures to safeguard the rights and freedoms of the data subjects , in accordance with Article 89(1) of the GDPR. By contrast, **in France**, Article 11 GDPR was assumed to refer to anonymised data. According to Chassang, the challenge is to ensure that the data are well anonymised. Individuals should be informed about the anonymisation and consequences regarding the exercising of their rights under the GDPR²⁷⁸.

Finally, **in Belgium**, two scenarios were considered:

- Where the data controller reusing data anonymises or pseudonymises the data itself, Article 11 does not prohibit informing the data subject prior to that reuse;
- Where the data controller who reuses data obtains anonymised or pseudonymised data from another party, Article 11 GDPR prohibits informing the data subject prior to that reuse.

In this case, the transparency obligation can be transferred to the original data controller through contractual agreements²⁷⁹.

6.2 Legal analysis of the application of the exemption to information duty for scientific research and appropriate measures under Article 14(5)(b) GDPR

6.2.1 Legal analysis of Article 14(5)(b) GDPR at EU level

The lawfulness of the processing operations is seriously endangered by the lack of a sufficient level of transparency on the use and further use of health-related data in the context of scientific research. Transparency allows data subjects to – *a priori*²⁸⁰ – learn about the planned data processing operations and – *a posteriori*²⁸¹ – enforce their rights. Additionally, where patients are able to find transparent information on the processing of their health-related personal data at the moment of their choice, they will find themselves (re-)assured and gain trust²⁸².

Prior to the implementation of the GDPR, participants in prospective (interventional) studies were generally informed about their privacy and the processing of their data through informed consent procedures. The CTD has harmonised the requirement for informed consent for participation in clinical trials using medicinal products. Since the GDPR, **it remains possible to inform data subjects about data protection through the informed consent form (ICF) for participation** in the clinical trial, on the condition that the structure of the ICF **clearly distinguishes** between (the risks caused by) participation and (risks caused by) data processing. Doing so is not advised where informed consent is not indicated as the legal basis for the data processing (see above), as it may cause confusion in data subjects and could potentially induce requalification of the legal basis.

Prior to the GDPR it was not uncommon to apply an exemption to transparency obligations for disproportionate effort. The size of the research project, the age of the data and the mortality rate in the research population were generally considered valuable arguments to allow researchers to provide information through **a public announcement** (website, leaflet, brochure, poster) rather than informing research participants individually. While such a public announcement **has little added value for data subjects**, the GDPR similarly allows for researchers to invoke disproportionate effort.

Currently, the exemption is restricted to situations where the data are not collected from the data subject²⁸³. It is necessary to clarify the distinction between Article 13 (data obtained from a data subject)

and Article 14 (data not directly obtained from a data subject).

In case of the further use of patient data (for scientific purposes), which article applies when the data have been collected directly from the patient by physician A, but are for the purpose of research reused by physician B, who is working in the same hospital but does not have a therapeutic relationship with the patient? When Article 14 is applicable, physician B could argue for an exception under Article 14(5)(b). When Article 13 is applicable, that physician would not be able to argue for an exception.

The importance of transparency might encourage restricting the scope of Article 14(5)(b). A two-step approach could be useful, especially in a context where data are further used **for more than one specific purpose** (e.g. more than one clinical trial, more than one research and development project, more than one project).

- In a first step, data controllers have to **provide general information to all** of the participants. In a hospital setting, this would mean that all ambulant and admitted patients are informed that research is conducted at the hospital. Transparency can be created by using patient information brochures, leaflets, websites, digital information screens;
- In a second step, the general information **should be supplemented with an individualised** overview of the projects and studies for which the data of that individual will be used. Such an overview should encompass prospective studies, retrospective studies and feasibility screenings (see definition of scientific research above). In a hospital setting, this would mean that on the patient portal of the hospital where the patient is treated, the patient is able to find an overview of the studies and clinical trials for which their data are used²⁸⁴. A complementary solution could be an EU portal providing a repository²⁸⁵.

6.2.2 Overview and analysis of national legislation and guidance on Article 14(5)(b) GDPR

The majority of countries investigated make no specific advice available. However, **France and Italy** have adopted a similar procedure - **authorisation is required from the DPA** prior to secondary use of personal data (including sensitive data) in cases where the controller (a third party) can rely on Article 14(5) GDPR.

In the UK, it appears that the lack of specific guidance likely results from the range of possible research circumstances to which the principle might apply and the need to consider the relevant processes and interests involved on a case-by-case basis²⁸⁶. In **Belgium**, the personal view of the researcher who contributed, has been reported above²⁸⁷.

Specific guidance (either in law or national guidelines) was reported in Germany, Hungary, Italy and France. In **Germany**, the Association for Data Protection and Data Security (GDD) made certain general observations on the concept of disproportionate effort. For example, the case-law findings that such an effort should not result from obstructions unnecessarily created by the controller, and cannot solely consider financial or organisational costs. The GDD eventually recognises that whether efforts are disproportionate or not can only be considered on a case-by-case basis²⁸⁸, given the range of possible research circumstances to which the principle might apply. In **France**, according to the CNIL²⁸⁹, all of the reasons mentioned in Article 14(5) GDPR can be invoked by the data controller to justify an exception to individual right to information in the context of scientific research. Nevertheless, this must be justified in detail by the controller. The controller will not have access to simplified procedures in these circumstances. CNIL authorisation is needed prior to the start of the processing. In each case, the CNIL assesses the reasons and circumstances of the exception invoked, as well as the guarantees presented by the controller (and processors) before providing any authorisation (assessment of the material difficulty in re-identifying the persons concerned, the human workload, the financial cost, the age of the data, the number of people, etc.). These assessments are performed with due consideration for the means available to the data controller to respect data subject's right to information. Where the

research project is submitted by law to a prior research ethics committee approval (for Research Involving Human Persons (RIHP) projects), the CNIL verifies that this has been obtained. In **Italy**, the Italian Data Protection Act (PDPC) contains a direct reference to the exemption to Article 14(5) GDPR. Pursuant to Section 110-a PDPC, secondary use of personal data for scientific research purposes by third parties is subject to authorisation by the SA, if informing the data subjects proves impossible or entails a disproportionate effort on specific grounds, or if it is likely to render impossible or seriously impair the achievement of the research purposes²⁹⁰.

6.3 ARTICLE 89(1) GDPR (OBLIGATION TO DE-IDENTIFY DATA COLLECTED) AND DATA SUBJECTS' RIGHTS UNDER THE GDPR

6.3.1 Legal analysis of Article 89(1) GDPR at EU level

Article 89(1) GDPR provides that processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall be subject to ‘appropriate safeguards’ of the rights and freedoms of data subjects. The nature of these appropriate safeguards is not clearly specified nor is it clear if national legislation may impose some specific measures or if the data controller alone can decide the appropriate safeguards. It could be argued that the principle of accountability and the lack of reference to margin of manoeuvre for the Member States in Paragraph 1 (although included in Paragraph 2) seems to indicate that the data controller is free to choose the more appropriate safeguards²⁹¹.

Article 89(1) GDPR only contains specific obligations for data minimisation. These specific obligations should be understood as a cascade obligation with three levels²⁹²:

- When, for the purpose of research, the use of personal data (that allow for the identification of the data subject) is not required, data should be anonymised²⁹³;
- When, for the purpose of research, the use of personal data (that allow for the re-identification of the data subject) is required, but the use of easily identifiable information including direct identifiers is not required, personal data should be pseudonymised²⁹⁴;
- When, for the purpose of research, the use of non-pseudonymised data, including direct identifiers, is required, an appropriate level of security should be achieved using different measures²⁹⁵.

When data are anonymised, the further use of data is out-of-scope of the GDPR. The sole question that arises in this case is whether the data subject must be informed about the anonymisation itself, since anonymisation is also a processing operation²⁹⁶. When data are transferred from one controller to another, it is the first controller that anonymises the data²⁹⁷.

When data are pseudonymised, the burden of the transparency principle is, in practice, often transferred to the party that collects the data – this is not necessarily the party that decides on the purposes and the means. For instance, in clinical research, the sponsor of the trial will determine the protocol (purpose and means of the research) and would be qualified as the data controller²⁹⁸. The participating site will collect the personal data, but as the data processor, because it does not determine the purpose and means. While the sponsor (controller) will provide the content of the information that needs to be provided to the data subject, the participating site (processor) will often be requested to provide the information to the data subject through the investigator. While the participating site should be free to claim compensation for their efforts, it seems correct that they are requested to provide the information to the data subject. This obligation should be included in the data processing agreement and in the study protocol.

To implement procedures to enhance transparency, ideas can be adopted from ICH GCP, especially the informed consent procedure (principle 4.8)²⁹⁹.

It could be argued that compliance with the transparency obligations under the GDPR can be achieved through a staged approach. Where it is necessary for the purpose of the research not to provide

information on the techniques and methodologies, a more general description should be allowed. Nevertheless, given that the GDPR does not provide for exceptions to the transparency obligation and the key role of this principle in the functioning of the GDPR, data controllers must ensure that data subjects are provided with additional information as soon as possible. Lessons can be learned from ICH GCP principles, for example, which apply to the use of single and double-blind studies.

The study sought to investigate how the transparency obligations under the GDPR apply in the context of projects using covert techniques. The GDPR contains no specific provision in this respect and few Member States have specific provisions or national guidance on the subject (see Section 5.3.2).

6.3.2 Overview and analysis of national legislation and guidance on Article 89(1) GDPR

In the majority of the countries examined, there were no insights into Article 89(1) GDPR³⁰⁰. **National advice** (in the form of law or guidelines) was found in **five Member States**³⁰¹. In **Germany**, the law provides certain legal clarification of the obligation to de-identify under Article 89(1) GDPR³⁰². There seems to be little further specific clarification of how these measures are to be implemented within specific research projects or organisations. This makes sense given the significant differences in types of research conducted, organisation of research approaches and resources available³⁰³. In **Slovakia**, similar to Article 89(1) GDPR, Section 78(8) DPA provides for general safeguards in cases of processing of personal data for scientific purposes. There is no direct reference to the possibility for third parties to access the de-identified data in the DPA or other legislation. In the case of the processing of data for scientific purposes, several data subjects' rights may be restricted (e.g. the right to access personal data, the right to rectification of personal data, the right to rectification of the processing of personal data and the right to object to the processing of personal data), as specified in Section 78(9) DPA³⁰⁴. In **Slovenia**, the **proposal** for a new data protection law includes a provision pursuant to which academic researchers registered with the relevant agency may under certain circumstances access previously processed data. This is permitted if they disclose certain information to the controller³⁰⁵. However, there is no certainty if or when the proposal will be adopted. Finally, in **the UK**, the Data Protection Act reiterates that the obligations outlined in Article 89(1) GDPR must be adhered to for the processing of personal data for research purposes. There is certain limited guidance available on the obligation to maintain principles of data minimisation in scientific research. The Health Research Authority, for example, states: '*Organisations must also have technical and organisational measures in place to ensure respect for the principle of data minimisation. These should include that only the absolute minimum amount or type of personal data required for a purpose is processed. Personal data should be pseudonymised where compatible with the research purpose, and identifiable data should not be used where the research purpose can be fulfilled by further processing with anonymised data*'³⁰⁶. The Authority notes, however, that this guidance will need to be implemented at organisational level³⁰⁷.

In **Bulgaria**, pursuant to Article 28(1) of the Health Act, **health information may be 'disclosed to third parties in any of the following cases: [...] 6. it is necessary for the needs of medical statistics or medical research, having deleted the data identifying the patient'**. The law does not specify whether 'deleting the data identifying the patient' is understood to mean pseudonymised or anonymised data. According to Opinion 05/2014 of the Article 29 WP, '*when a data controller does not delete the original (identifiable) data at event-level, and the data controller hands over part of this dataset (for example after removal or masking of identifiable data), the resulting data is still personal data*'³⁰⁸. There appears to be no specific guidance in Bulgarian case-law/codes of conduct on the technical measures required to comply with Article 28(1) of the Health Act. It can likely be assumed that in most cases the data disclosed would be pseudonymised data, i.e. personal data. This issue touches on the complex discussion about absolute/relative anonymisation, which is not yet solved at EU level³⁰⁹. Currently, there is no consistency at national level or in international standards as to what constitutes anonymisation³¹⁰.

6.3.3 Overview and analysis of national legislation and guidance on projects using covert techniques

There was no specific law or national guidance available in the majority of the countries investigated (13 out of 18)³¹¹. In France, a specific article for ensuring ethical deception practice in research **limits the use of deception to the sole research in psychology** (explicit purpose limitation; and explicit mention of the type of information exceptionally allowed to be hidden from the participant, see Article L. 1122-1 PHC). The practice of deception method, even if scientifically justified, in no way entirely deprives research participants of their right to be informed. The information process will nevertheless be adapted before the first data collection and completed as soon as possible afterwards. Complete information on the research is provided at the end. The use of deception and its justification from a scientific or methodological point of view shall be detailed in the dossier submitted to the competent REC (*Comité de Protection des Personnes*, mentioned in Article L. 1123-6) and explicitly mention the nature of the preliminary information sent to potential research participants. The REC will assess and approve or reject such a possibility, on a case-by-case basis. Correct implementation of the approved procedure should be documented by the data controller during the research as part of its accountability obligation. In Belgium, the national input for this study echoes the rationale of the French law, i.e. that the use of covert techniques should not prevent researchers from being completely transparent at the end. Once the study is complete, data subjects should be further informed³¹².

7 POLICY RECOMMENDATIONS

Chapter 7 presents some approaches and policy recommendations to better harmonise the legal regime relating to scientific or historical research or statistical purposes. Section 7.1 presents general recommendations and Section 7.2 more specific recommendations.

7.1 GENERAL RECOMMENDATION: INCREASED DIALOGUE AND COOPERATION

There is no uniformity in Member States' approaches to key aspects of the secondary use of personal data for scientific research. Following the detailed analysis presented, the **general recommendation is for the EDPB to encourage increased dialogue between Member State SAs, sharing of information** on national practices and interpretations in view of Article 60 and following the GDPR, and **cooperation** between Member State SAs, European institutions and bodies, and key stakeholders.

In addition:

- The **EDPB and other European institutions and bodies** (European Commission, EDPS, regulatory bodies in the research field, such as the EMA) could establish closer exchanges, with a view to aligning their advice on the interplay of the GDPR and other sectoral laws (CTR, national biobank legislation, etc.). Discrepancies are evident in the views of European institutions and an alignment of positions would greatly aid practitioners (such as commercial and academic research institutions) in applying the GDPR.
- The **EDPB could promote** the establishment of relevant sectoral **codes of conduct** (as per Article 40 GDPR), such as that currently drafted by the Biobanking and BioMolecular Resources Research Infrastructure – European Research Infrastructure Consortium (BBMRI-ERIC) in the sphere of health research. This can be done via official communication.
- The **EDPB could stress** the importance of involving **all key stakeholders** (commercial and academic research centres, patients, consumers, governments and citizens) in the creation of sectoral codes of conduct and binding and non-binding guidelines. Empirical research on a pan-European scale could be useful in mapping stakeholders' experience, challenges and solutions.
- The **EDPB could adopt guidelines to address the secondary use of personal data for scientific research** (see Section 6.2 for specific areas needing guidance). A distinction could be made between: (i) problems caused by a lack of uniformity in the interpretation of the key elements of GDPR and (ii) divergences in Member States' implementation of the margins of discretion in the GDPR in national laws.

7.2 SPECIFIC RECOMMENDATIONS

Table 6 presents some suggested approaches to topics that should be addressed in future EDPB guidelines on the topic of secondary use of personal data for scientific research purposes. These recommendations reflect the findings of the study, particularly with respect to health data. The table notes whether the problems are caused by a lack of uniformity in interpretation ('interpretation issue') or divergences in the implementation of the GDPR in national laws ('implementation issue'). In certain cases, both types of issue are evident.

Table 6: Suggestions for the EDPB guidelines on secondary use

No	Topic	Interpretation or implementation issue	Findings	Recommendations for the guidelines
1	Importance of international agreements and documents	N/A	Data protection for secondary use of health data should be interpreted in the light of international documents, conventions and recommendations.	Clarify the importance and influence of international documents, conventions and recommendations with regard to the role of research, public interest and reasonable expectations in case of secondary use of personal data, especially in the medical domain.
2	Notion of scientific research	Interpretation issue	The GDPR neither defines nor provides clear guidance on the substantial elements of what it intends by scientific research. Most Member States do not specify the topic any further in their national legislation.	Invite Member States' SAs to cooperate in (i) sharing and discussing the substantial characteristics of what could be considered scientific research, and (ii) defining the research that should fall under the GDPR terms. These characteristics should be systematised in EDPB guidelines.
3	Notion of secondary use	Interpretation issue	The term 'secondary use' is not an established term used in EU general data protection legislation. The term is quite recent and increasingly used, in particular in national legislation, e.g. Finland.	Discuss the concept of 'secondary use' in relation to the concept of 'further processing of data', and describe and define the term.
4	Legal basis, secondary use and choice	Both	Although much-debated, a legal basis remains required, including where personal data are further processed for research purposes. For presumed compatible research purposes, this could be the same or a new legal basis. At the same time, due regard shall be given to the nature of the data (Article 9 GDPR).	Clarify that a legal basis remains required, including where personal data are further processed for research purposes, which could be the same or a new legal basis.
4.1	Choice of legal basis (Article 6 and Article 9 GDPR)	Interpretation issue	The analysis of the national responses highlights that few countries see Articles 6 and 9 GDPR as separate requirements (non-cumulative requirements). Two countries see them explicitly as alternatives and the majority have no official position. There is no harmonised position between Member States.	Insist on a common position so as to ensure legal certainty in respect of the objective of the GDPR that aims at common data protection standards throughout the EU and EEA.
4.2	Choice of legal basis (considerations for pan-European studies)	Both	There are considerable differences at national level when it comes to the legal bases used when processing personal data in the context of medical studies, for example. These differences hinder transnational studies (e.g. a clinical trial with investigation sites open in several countries).	Offer guidance on how to reconcile the use of preferred but different legal bases in transnational studies.
4.3	Public interest	Both	Doubt remains on the use of the legal basis of tasks in the public interest allowing 'compatible' scientific research, at least in the clinical trials context. In addition, Article 6(1)(e) GDPR may not be the best fit for transnational studies.	Offer guidance on the conditions under which Article 6(1)(e) GDPR is a legal basis that suits research institutions operating at national level. Support investigations into the clarification of the notion 'public interest' across EU Member States.

No	Topic	Interpretation or implementation issue	Findings	Recommendations for the guidelines
			The notion of ‘public interest’ appears to play a central role in all of the main justifications under Article 9(2) GDPR.	
4.4	Legitimate interest	Interpretation issue	<p>The reasonable expectations of data subjects will be important, at least when relying on legitimate interests but also for the assessment of the research being ‘compatible’ (secondary use).</p> <p>Article 6(1)(f) GDPR is a legal basis that could be invoked by private or commercial research institutions provided there remains a balance with the rights and freedoms of data subjects, which shall at all times be verified. Ethics committees could play a role in clarifying the balance of interests.</p>	Offer additional guidance on the conditions under which Article 6(1)(f) GDPR is a suitable legal basis for secondary use for research.
4.5	Broad consent	Interpretation issue	<p>Key issues are (i) whether or not broad consent could stretch compatible processing for research from ‘primary use’ to ‘secondary use’, including in the clinical trial context, and (ii) the meaning of the words ‘certain areas of research’ in Recital 33 GDPR.</p>	Clarify the role of broad consent on the two issues mentioned.
5	Legal basis and purpose limitation	Both	<p>Specific legal grounds could be invoked other than consent, insofar as specific conditions are met for compatible research. As it is likely that not all research outside earlier defined projects (e.g. clinical trial) may meet these conditions, including the expectations of individuals and society, debate should be encouraged about the preferred ground (if such preference is to be established). Agreement by the data subject (consent) would be suitable in some cases but not feasible or possible in others.</p>	Obtain the positions of SAs and offer additional guidance in this regard.
6	Data subjects’ rights			
6.1	Explicit consent	Both	<p>The analysis highlights that there is some homogeneity in the distinction between consent to the data processing and consent to the research, but no binding advice. Evidence suggests that, in practice, researchers and study participants may not distinguish between the two types of consent.</p>	The EDPB should stress the importance of information and training for stakeholders regarding the distinction between consent for participation and consent under the GDPR.
6.2	Projects using deception/covert techniques in research	Interpretation issue	<p>Only France has provided specific rules for the ethical use of deception in research and the limitation to the duty of information.</p>	Invite Member States to adopt a harmonised position. This can be inspired by the French example, i.e. the use of deception should be (i) limited to a specific field (i.e. psychology), (ii) justified, (iii) approved by an ethics committee on a case-by-case basis, and (iv) the data controller should be fully transparent

No	Topic	Interpretation or implementation issue	Findings	Recommendations for the guidelines
				to data subjects at the end of the research study.
6.3	Article 11 GDPR	Interpretation issue	A major issue is how Article 11 GDPR fits with the transparency obligation and rights to information of data subjects, including in particular Article 14(5)(b) GDPR. In the case of controller-to-controller transfer, there is a risk of depriving data subjects of their fundamental right to fairness of data processing. The above risk to fairness could be argued to raise concerns for health or genetic data.	Consider choice for the data subjects and other means to respect transparency, such as agreements between controllers to inform data subjects (e.g. Belgium).
6.4	Article 89(1) and data subject rights (including Articles 13-14 GDPR)	Interpretation issue	No insights were available in the majority of investigated countries with respect to the application of Article 89(1) of the GDPR.	Invite Member States to adopt a harmonised position, which could usefully be inspired by the ICH GCP principles.
6.5	Article 14(5)(b) GDPR	Interpretation issue	Little specific advice is available at national level. Two countries (France and Italy) require authorisation from the DPA prior to further processing of personal data (including sensitive data),	Consider a two-step approach to restrict the scope of Article 14(5)(b) GDPR: <ul style="list-style-type: none"> ▪ In a first step, data controllers have to provide general information to all of the participants; ▪ In a second step, the general information should be supplemented with an individualised overview of the projects and studies for which the data of that individual will be used.
6.6	Appropriate safeguards	Interpretation issue	An analysis of the safeguards looked at the concept of information and access in connection with Article 89(1) GDPR. No insights were available in the majority of countries. National advice (in the form of law or guidelines) was found in four EU Member States. There is no conclusive answer on whether or not Member States alone are allowed to determine the appropriate safeguards, or whether the data controller can decide.	Address what can be considered ‘appropriate safeguards’. It is important that SAs cooperate more closely and exchange information on national perceptions of appropriate safeguards, e.g. the use of contractual arrangements.
7	Ethics committees role	N/A Ethics committees are not discussed in the GDPR	There is evidence that ethics committees often advise on data protection matters (e.g. legal basis for the processing of personal data). A suitable role for ethics committees under the GDPR could be in	Clarify the distinct roles of ethics committees, DPOs and SAs. More empirical analysis and study could be useful in this respect.

No	Topic	Interpretation or implementation issue	Findings	Recommendations for the guidelines
			risk assessment, particularly in the balancing exercise foreseen in Article 6(1)(f) GDPR.	

8 CONCLUSIONS

This study investigated pertinent questions about the secondary use of personal data for scientific research. Based on the information gathered on 18 countries, there appears to be a lack of a uniform approach among Member States. This might lead to a lack of protection of data subjects involved in research, or ‘forum shopping’ for commercial actors undertaking scientific research.

The diversity of positions reflects the margin of manoeuvre left to Member States by the GDPR, with respect to the processing of personal data in the framework of research. Equally, the GDPR itself is not explicit on some points. This study shows that the situation and laws in the Member States are different because some have specific national provisions clarifying the European legislation.

The first concern is the meaning of ‘scientific research’ - there is no clear definition in the GPDR and most Member States do not specify it further, except in some sectoral laws. Without a clear definition, homogenous application of the presumption of compatibility and the Article 89 GPDR specific framework is not possible.

The terms ‘secondary use’ and ‘further processing of data’, and the links between them, need attention and guidance to prevent misunderstandings. In the case of reuse of personal data, the question of the need for a (new) legal basis should be clarified, given that some Member States require a new legal basis while others do not. Similarly, Member States lack a clear position on legal bases for sensitive data, with little clarity on the articulation between Articles 6 and 9 GDPR (cumulative requirements or separate requirements). Few Member States clearly see Article 9 GDPR as a cumulative requirement. The choice of legal basis can also pose a problem for pan-European studies.

The effectiveness of data subjects’ rights was an important aspect of the study, especially in relation to consent and the right to information. Some clarifications seem necessary, for instance in relation to application of the transparency obligation in cases of reusing personal data, or how precisely data subjects may choose the areas of scientific research where their data could be used (interpretation of Recital 33 of the GDPR).

Questions remain about the concept of ‘appropriate safeguards’ in the context of Article 89 GDPR. Most Member States lack clear practical guidance on the kinds of measures that should be implemented by the data controller. Another concern is the possibility for Member States to impose some specific measures in this context.

It seems clear that the EDPB could usefully promote cooperation and dialogue between SAs and between different European institutional bodies involved in scientific research regulation with a view to providing these clarifications.

The promotion of sectoral codes of conduct (binding on adherents) or guidelines is another possible solution. These kinds of instruments should be developed with input from a large panel of stakeholders (commercial and academic research centres, patients, consumers, governments and citizens).

Even if clarifications are provided by EDPB guidelines, or codes of conduct, national differences may persist due to national law rather than interpretations of GDPR provisions. In such cases, the EDPB would have limited ability to harmonise these rules and the only way forward would be to modify EU or Member State legislation.

Finally, the GDPR overlaps and interacts with other specific European legislation (CTR, Biobanks Directives). Further guidance on the interplay between these different pieces of legislation could be beneficial.

ANNEX 1 – FIGURES AND TABLES

Figure 1: Schema on the primary use and secondary use of data

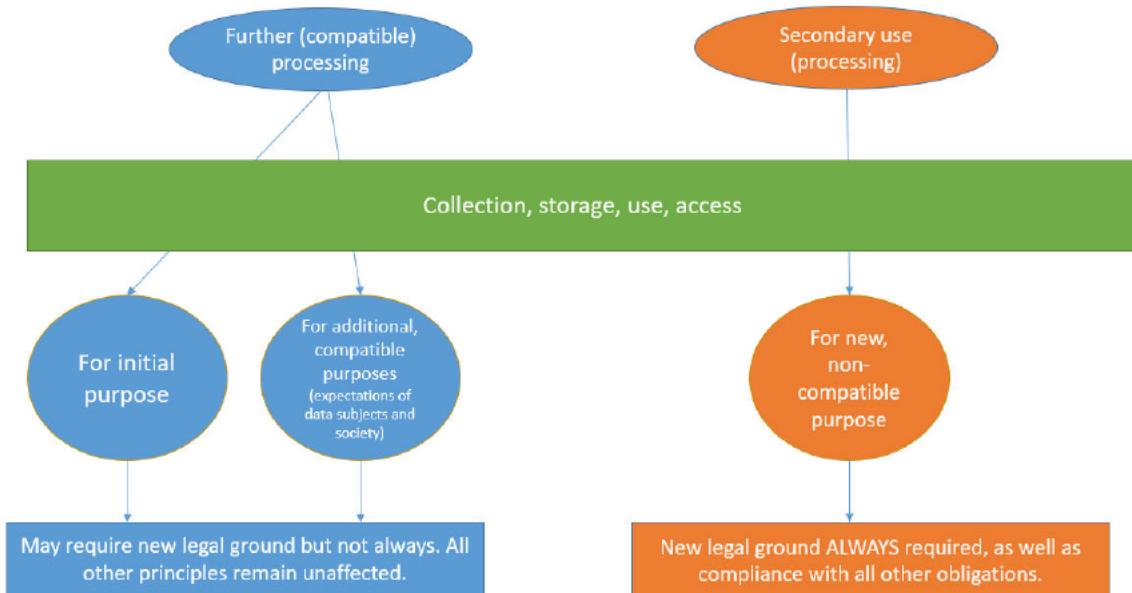


Table 1: Definition of scientific research in national legislations

Categories Country	Umbrella definition of 'scientific research' in national legislation	Umbrella definition of 'scientific research' in national case-law	Definition of 'scientific research' in legislations related to the health sector, the medical sector, or the public sector	Definition of 'scientific research' in soft law related to the health sector, the medical sector, or the public sector
Belgium			Law of 7 May 2004 "Wet inzake experimenten op de menselijke persoon", Article 2(7) and Article 2(11)	
Bulgaria	<u>Promotion of Scientific Research Act, Article 1(9)</u>		<u>Health Act, Article 197(2)</u>	
Croatia				
Cyprus				
Denmark	No definition but the study has to be of 'a significant importance to society' if it concerns Article 9 GDPR data (Article 10 Act No. 502 of 23 May 2018)			

Categories Country	Umbrella definition of 'scientific research' in national legislation	Umbrella definition of 'scientific research' in national case-law	Definition of 'scientific research' in legislations related to the health sector, the medical sector, or the public sector	Definition of 'scientific research' in soft law related to the health sector, the medical sector, or the public sector
France	French Code of Research, Article L.112		French Public Health Code, Article L.1121-1	
Germany		BVerfGE 35, 79, 112 and BVerfGE 47, 327, 367		
Greece	Law 4310/2014 on Research & Innovation, Article 2(4) and Law 4386/2016 on Rules of Research, Article 2(4) (exact same definition)		Law 3418/2005 on Medical Conduct, Article 1(2)	
Italy			Decreto Legislativo 30 dicembre 1992, n. 502 Riordino della disciplina in materia sanitaria, a norma dell'articolo 1 della Legge 23 ottobre 1992, n. 421. Art 12	
Latvia			Law on Scientific Activity, Art. 1, and The Pharmaceutical Law, Article 1 and The Human Genome Research Law, Article 1	
The Netherlands			Medical Scientific Research with People Act, Article 1.1	Foundation Federation of Dutch Medical Scientific Societies - Self-regulatory code of conduct for Observational Research with personal data
Portugal			Decree-Law No. 63/2019, of 16 May, on the scientific research and technological development institutions (R&D) and Law no 21/2014, of April 16, on clinical research	
Romania	Governmental Ordinance No. 57/2002, Article 2(1)			

Categories Country	Umbrella definition of 'scientific research' in national legislation	Umbrella definition of 'scientific research' in national case-law	Definition of 'scientific research' in legislations related to the health sector, the medical sector, or the public sector	Definition of 'scientific research' in soft law related to the health sector, the medical sector, or the public sector
Slovakia			Act no. 172/2005 Coll., Art.2 and Act no. 576/2004 Coll., Article 12	
Slovenia	Research and Development Activities Act, Article 5			
Norway			Health Research Act, Chapter 1, Section 4(a)	

Table 2: Explicit consent requirements for personal data processing in case of scientific research

Categories Country	Type of the binding / non-binding instrument	Name and hyperlink of the binding / non-binding instrument	Short description
Belgium	Non-binding informed consent templates	Informed consent templates as foreseen by the Clinical Trial College (CTC)	The informed consent template is recommended to researchers, while not compulsory. It prompts the researchers to provide information on the legal basis for the processing and the type of data collected, prohibits the researchers to make available the identity of the participant to the sponsor and in publications, obliges them to use 'coded' data and sets out what happens with the results of their studies. The CTC is an initiative of the Belgian Federal Government in which all medical ethical committees are involved.
France	SA issued methodology	CNIL Methodologies of Reference	The CNIL has adopted five reference methodologies. The first one, i.e. MR-001, provides a secure framework for research involving human persons (RIHP) requiring explicit consent under the rules of the French Public Health Code. This consent should not be interpreted as consent referred to within the GDPR. Nevertheless, it is common that both type of legal basis be confounded by health professionals and lawyers.
Greece	Template for Code of Ethics	Template Code of Ethics for research in biological sciences by the National Bioethics Commission	In order to facilitate the work of research institutions, the National Bioethics Commission has issued since 2008 a (non-binding) template with the basic principles of deontology and ethics which should govern biological research. Based on this template, in the case of clinical trials (Article 12), research on human biological materials (Article 13) and research on human embryos (Article 14), researchers are asked to pay particular attention and adhere to generally applicable principles, including informed consent, as well as to comply with the legal

Categories Country	Type of the binding / non-binding instrument	Name and hyperlink of the binding / non-binding instrument	Short description
Italy	SA's decision	Processing of health data for research purposes Decision of 5 June 2019	<p>provisions covering processing of (sensitive) personal data protection.</p> <p>In Paragraph 4, the <i>Garante</i> sets the requirements on processing of genetic data for research purposes. The decision foresees that consent is required for the processing of genetic data for scientific research purposes that are not regulated by law or other requirement set pursuant to Article 9 GDPR. In addition, it sets many requirements concerning consent for processing genetic data for research purposes. Moreover, in Paragraph 5, the <i>Garante</i> confirmed consent as a legal basis, where law or regulation as legal basis does not apply.</p>
	SA's decision	Ethical standards for statistical or scientific research processing activities Decision of 19 December 2018	<p>These deontological rules apply to all the processing activities carried out for statistical and scientific purposes by universities, other research bodies or institutes and companies, as well as researchers who work in the context of said universities, institutions, research institutes and members of said scientific societies. They do not apply to processing for statistical and scientific purposes connected with the protection of the health performed by health professionals or health bodies, or with comparable activities in terms of significant personalized impact on the interested party, which remain regulated by their relevant provisions, also at local level.</p>
The Netherlands	Code of Conduct	Foundation Federation of Dutch Medical Scientific Societies: Self-regulatory code of conduct for Observational Research with personal data	<p>Article 4(1) of the Code of conduct for Observational Research with personal data: Subject to the provisions of chapters 5 and 6, personal data may be processed for research only if the data subject has expressly given his consent (unofficial translation).</p>
	Professional Guidelines	Royal Dutch Medical Association (KNMG), 'Guidelines for dealing with medical data'	<p>Paragraph 5(11) of the Guidelines for dealing with medical data: Main rule for disclosing personal patient data for scientific research or statistics, is that the patient must give explicit consent. There are exceptions for this main rule if asking for consent is not possible or cannot be required from the doctor, and additional conditions are completed (unofficial translation).</p>
Portugal	Law	<p>Law no. 58/2019 ensuring execution, in the national legal order, of Regulation (EU) 2016/679</p>	<p>This law does not mention clearly the possibility to process data without consent.</p>
Romania	SA's Guide	Guide on Questions and Answers on the Application of	<p>Under the question 21. 'What are the conditions for giving consent and its validity?', the SA provided, among others conditions, the following</p>

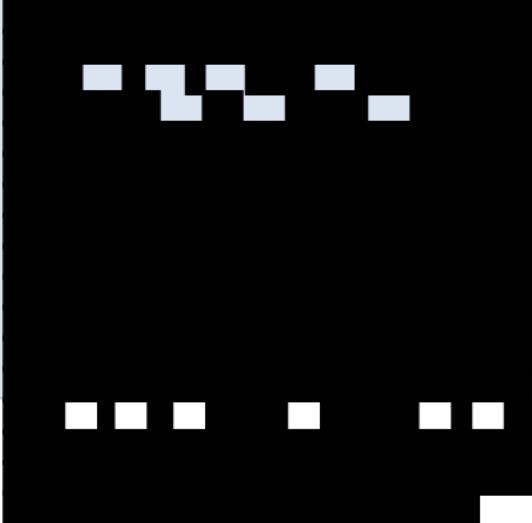
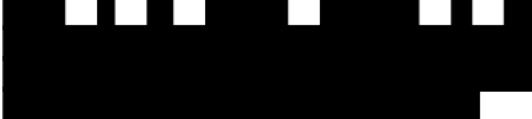
Categories	Type of the binding / non-binding instrument	Name and hyperlink of the binding / non-binding instrument	Short description
Country			
		Regulation (EU) 2016/679	answer: “The consent must cover all processing activities carried out for the same purpose or for the same purposes. If the data processing is done for more purposes, consent must be given for all purposes of processing”. Under this question, the SA does not mention that processing of personal data would be allowed for scientific research purposes without the consent of the data subject. However, there is no indication that Articles 9(2)(a) and 9(2)(j) of the GDPR should not apply. Under question 20. What are the conditions for processing of special categories of data?, the SA lists the provisions of Article 9 of the GDPR.
	SA's Statement	Processing of personal data concerning health in the context of the COVID-19 pandemic (March 2020)	The SA published a statement on its website with regard to the processing of health data, recommending the operators to consider the general GDPR provisions related to the conditions of processing health data, highlighting points a), b), h) and i) of Article 9 of the GDPR. The SA also specified that personal data, other than those of a special category, can be processed in compliance with Article 6 GDPR. Regarding the disclosure in the public space of the name and state of health of a natural person, the SA emphasized that the processing (disclosure) of these data can only be done with the consent of the person concerned.

Table 3 : Need for a separate legal basis for secondary use of personal data for research

Who	Is a new legal basis needed?		
	Yes	No	Maybe
EDPB			✓
EDPS	✓		
European Commission			✓ The new lawful ground may or may not differ from the legal basis of primary use.
European Parliament (not official view, but in a report prepared for the STOA panel)	Not discussed	Not discussed	Not discussed
EMA		✓	
GDPR commentary (Oxford University Press 2020)	✓		
GDPR Commentary (Elgar Forthcoming 2021)		✓	
ISC seminar (stakeholders views) ³¹³		✓	
EORTC			✓ Possibility to continue with

Who	Is a new legal basis needed?		
	Yes	No	Maybe
			a new basis, not an obligation.

Table 4: Medical secrecy national rules

Country	Interesting quotes/personal opinions from the desk research	Legal provisions, codes of conduct, opinions and others, if identified
Belgium		
Bulgaria		<p>Pursuant to Article 54 of the Code of Professional Ethics of Medical Doctors, data and illustrations which are subject to medical secrecy may be communicated for the purposes of scientific activities only if the anonymity of the patient is guaranteed. Moreover, patients should not be identified by third parties.</p> <p>Pursuant to Article 25(2) of the Code of Professional Ethics of Dentists, <i>"all facts and circumstances of the patient's personal life which became known to the dentist in his professional activity and have been included in the patient's medical file, are confidential and not subject to disclosure except in cases provided by law or with the written consent of patient"</i>.</p> <p>The unlawful disclosure of any type of professional secret is criminalized in Article 145 of the Criminal Code.</p> <p>Opinion № II-2882/2013 from 11.06.2013 of the Bulgarian DPA. The Opinion concerns sharing of data of diseased persons for the purposes of a PhD study. Under the old Data Protection Act, such data was considered personal data, therefore it may provide an interesting point of discussion with respect to secondary use of personal data for research purposes. The CPDP found that while such data cannot be shared by the Bulgarian Integrated information system for demographic statistics (ESGRAON), it can be disclosed by a hospital. Among the main considerations of the CPDP were the obligation to conduct scientific research to which a doctoral researcher is</p>

Country	Interesting quotes/personal opinions from the desk research	Legal provisions, codes of conduct, opinions and others, if identified
		subject pursuant to Article 6(3) of the Higher Education Act and the fact that the doctoral researcher in the specific case was also a medical professional and would be processing the requested personal data in his professional capacity, meaning that he would be under the obligation to protect professional secrecy.
France		Article 68 LIL Article 74 LIL
Germany		The <i>Musterberufsordnung für Ärzte 2015</i> – the Code of Conduct for Doctors; confidentiality duties in Article 203 of the <i>Strafgesetzbuch (StGB)</i> – and the Criminal Code; confidentiality duties in Article 35 of the <i>Sozialgesetzbuch I (SGB I)</i> – book 1 of the Social Code
Italy		<p>2014 Medical Deontological rules</p> <p>Article 10: “<i>The doctor shall ensure the ‘non-identifiability of the involved subject in the context of scientific publication of medical studies or clinical trials</i>” and “<i>the doctor shall not collaborate in the establishment, management or use of databases of assisted persons in the absence of guarantees on the preliminary acquisition of their informed consent and on the protection of the confidentiality and security of the data</i>”.</p> <p>Article 78: “<i>The doctor, in the use of information and communication technologies for prevention purposes, diagnosis, treatment or clinical surveillance, or such as to affect human performance, adheres to proportionality, appropriateness, efficacy and safety criteria, respecting the rights of the person and application addresses attached</i>.”</p>
The Netherlands		

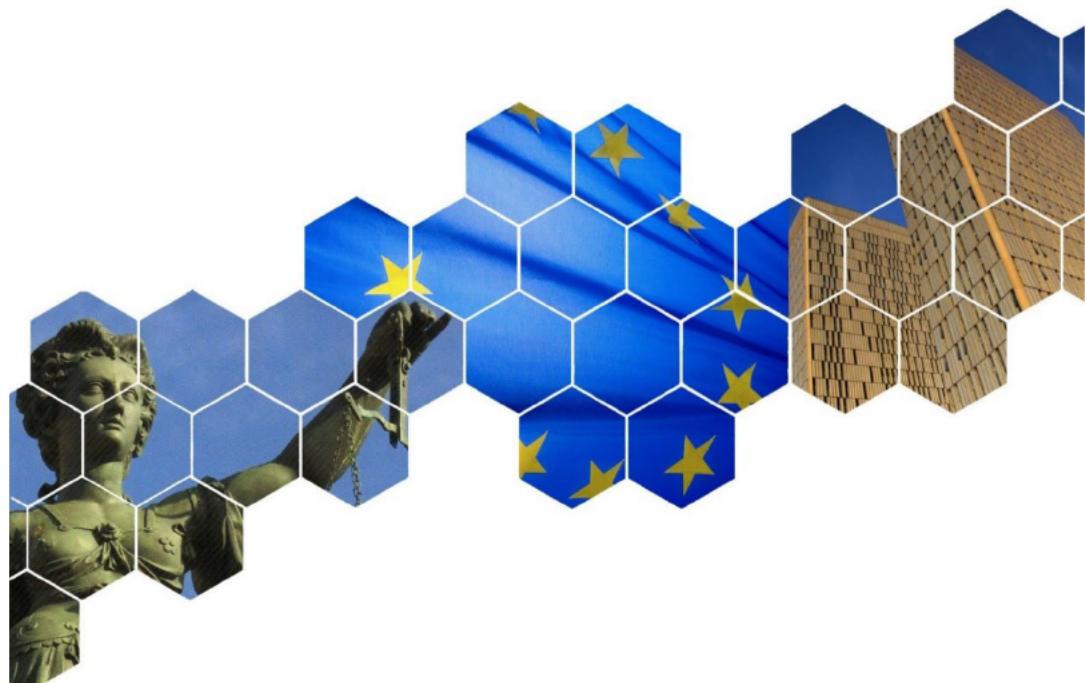
Country	Interesting quotes/personal opinions from the desk research	Legal provisions, codes of conduct, opinions and others, if identified
Portugal	[REDACTED]	Article 29(2) of Law No. 58/2019

ANNEX 2 – QUESTIONNAIRE ON RELEVANT NATIONAL LAWS AND PRACTICES¹

¹ This questionnaire was intended for external use. Questionnaire used by internal researchers was slightly more elaborate.

Secondary use of personal data in the context of scientific research

Questionnaire on relevant national laws and practices



BACKGROUND INFORMATION

The European Data Protection Supervisor (EDPS) and the European Data Protection Board (EDPB) recently awarded a framework contract for ‘Studies on the implication of several GDPR provisions, case laws and other laws having an impact on data protection’. This questionnaire on secondary use of personal data for scientific research is provided within this framework contract **and shall be kept strictly confidential**.

This questionnaire is aimed at compiling relevant legal information about national regulation and on secondary use of personal data for scientific research the implementation of specific provisions of the GDPR by EU Member States and EFTA EEA countries (Iceland, Lichtenstein and Norway).

We would like to obtain an overview of the applicable national legislation, guidelines, decisions and conditions for the secondary use of personal data for scientific purposes, with a specific focus on how the principles of purpose limitation and lawfulness, which are closely related when it comes to the secondary use of personal data, are applied in the context of scientific research. This Questionnaire has been designed as a methodological tool to gather national information from experts on the national specificities.

Please provide answers to all questions which are relevant in the context of your national legal order. When we ask for explanation on the national rules, please consider also case law, legal interpretation by legal scholars and any national guidelines from the SAs and other relevant authorities, (legal) scholar views and national practices that are relevant. Please provide with your answer any relevant specific source, including links or attachments to the relevant sections or legislation pieces.

We would be grateful to receive your input by June 8. If you would need more time, please let us know in advance so that we can take this into account. Once completed, please send it back to [REDACTED] and eleftherios.chelioudakis@kuleuven.be. If you have any questions regarding this study or the questionnaire, please contact the same e-mail addresses.

Data Protection Notice

Please be informed that all personal data that you provide by collaborating and answering to this questionnaire and gathered for this study - in particular your contact details and your input to the questions - will be treated in conformity with Regulation (EU) 2018/1725 and all other applicable legal requirements.

The controller for execution purposes of the procurement framework contract, including the conduct of the legal studies, is the EDPS (including the EDPB Secretariat) and the EDPB.

Your personal data will be processed by the consortium of partners, including their subcontractors/affiliates, namely Milieu Consulting SPRL, the Center for Law and Digital Technologies (eLaw) from Leiden University, KU Leuven, represented by the KU Leuven Centre for IT & IP law (CiTiP), the Research Centre in Information Law and Society (CRIDS) from the University of Namur and CLI - Vrije Universiteit Amsterdam, acting as processors on behalf of the EDPB and the EDPS and under their sole instructions.

The content of your replies you provide will be used by those processors to gather information and knowledge for the provision of the report. Your answers will remain confidential, and will not be transferred to any other third parties, except where legally required (e.g. audits by EU bodies or access to documents requests, on the basis of available exceptions and in accordance with applicable law).

No responses to the questionnaire will be published with any of your contact details. Please note, however, that, at your request, a general reference to your full name and/or professional affiliation as a participating expert may be included in the study. Should that be the case, please make such request, in writing, to the consortium as an expression of your consent. Such reference will become public in the event that the study is published or made accessible following an access to document request. You may withdraw your consent at any time, but please note that all activities carried out before your withdrawal remain lawful.

For information on how your personal data will be processed in the context of these activities, including on the applicable legal basis and retention periods applicable to the processing of your personal data, on the exercise of your data subject rights and the necessary contacts concerning complaints, please read the applicable EDPB / EDPS data protection notice on the execution of the contract.

For information on how your personal data will be processed in the context of the management of the contract, please check the EDPS data protection notice: https://edps.europa.eu/data-protection/our-work/publications/other-documents/12-edps-data-protection-notice-procurement_en.

Confidentiality clause

Please treat in the strictest confidence and do not make use of and do not divulge to third parties any information or documents, disclosed in writing or orally, which are linked to the performance of this study, including the questionnaire and the name of the study, unless:

- The use is required to answer this questionnaire;
- The EDPB gives you our prior written consent to the disclosure;
- You are required by law or by any regulatory authority to make the disclosure; o
- The document or information has entered the public domain other than by wrongful disclosure by you.

Please note that you shall continue to be bound by this obligation after completion of this questionnaire without limit in time.

QUESTIONNAIRE

Contact details

Contact persons and contacts

Please, provide your name and your position within your organisation:

Please, provide your contact information (e.g. email and/or telephone number):

I. General questions

1. Is “scientific research” defined in your national legislation (*lex generalis* or *lex specialis*, e.g. health legislation) and/or does the national legislation or case law in your country list principles that define scientific research? Please, bear in mind that specific arrangements can exist for a specific type of research (e.g. medical research), hence information should be looked for not only in general law, but also in sectorial legislation.

(Please also provide reference to the applicable legal act and article, if any; feel free to use more space if needed)

2. If there is no legal definition, are you aware of case law, sectorial guidance, case law or any other source that provides a commonly accepted definition or is there a specific understanding of scientific research in your country ?

II. Implementation of the principle of lawfulness of processing of *special categories of personal data* for scientific research in your country under 9(2)(a)² and Article 9(2)(j)³ of GDPR.

1. Are there national legal provisions which require “explicit consent” as under Article 9(2)(a) GDPR for scientific research in your country, and in which contexts ?

(Please also provide reference to the applicable legal act and article, if any; feel free to use more space if needed)

2. Are you aware of case law, codes of conduct, SA guidelines, other binding or non-binding instruments and/or practices in your country that impose the use of “explicit consent” in the context of scientific research?

(Please also provide reference to the applicable legal act and article, if any; feel free to use more space if needed)

² Article 9(2)(a) GDPR: “The data subject has given explicit consent to the processing of those personal data for one or more specified purposes...”.

³ Article 9(2)(j) GDPR : “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”.

3. How is consent as lawful ground in your country understood in the light of (and in combination with) Regulation 536/2014 on clinical trials⁴ ?

(Please provide detailed answers, e.g., is it regulated in a legislative act? Does any case law, SA or sectorial guidance or scholarly views on this matter exist? What is your first analysis on this topic?)

III. Implementation of the principle of lawfulness and purpose limitation for the processing of *any category of personal data (both special and non special categories)* as applied in the context of scientific research

1. How is consent as lawful ground in your country understood in the light of recital 33 GDPR⁵ ('consent to certain areas of scientific research' ('broad consent')) ?

(Please provide detailed answers, e.g., is it regulated in a legislative act? Does any case law, SA or sectorial guidance or scholarly views on this matter exist? ...What is your first analysis on this topic?)

2. Is there a distinction between the use of consent as lawful ground

(Please provide detailed answers, e.g., is it regulated in a legislative act? Does any case law, SA or sectorial guidance or scholarly views on this matter exist? ...What is your first analysis on this topic?)

- for *primary use* of data in light of recital 33 GDPR ?

- for *secondary use* of data ?

3. Do your *national laws* provide for an appropriate lawful ground for the processing of personal data in the context of scientific research, including secondary use of personal data as provided under Article 9(2)(j) of the GDPR?

No []

Yes []

Name of the national legislation and hyperlink (if possible)	Details of the Article (Number, paragraph)	Description of the Article

⁴ Regulation 536/2014 on clinical trials on medicinal products for human use. Available [here](#).

⁵ Recital 33 GDPR: "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".

--	--	--

4. Does your country has any rules/guidance/case law, scholarly views with respect to whether a new lawful ground is required for secondary use of data ?

(Please provide detailed answers, e.g., is it regulated in a legislative act? Does any case law, SA or sectorial guidance or scholarly views on this matter exist? ... Please included references. What is your first analysis on this topic?)

IV. Implementation of the principle of purpose limitation for the processing of *any category of personal data* (both special and non special categories) as applied in the context of scientific research

1. About the implementation of the “presumption of compatibility”⁶ for the secondary use of personal data for scientific, historical and statistical purposes (Article 5(1)b):

- How does this principle apply in your country?

(Please provide detailed answers, e.g., is it regulated in a legislative act? Does any case law, SA or sectorial guidance or scholarly views on this matter exist? ... Please included references. What is your first analysis on this topic?)

- Is there any case law, scholarly views, national guidelines describing how this principle is implemented and interpreted by relevant authorities in your country (for example, in cases when the personal data was initially collected in the scientific research context or not)?

No []

Yes []

Title of the document and hyperlink	Description on how this principle is implemented and interpreted

2. How is such presumption of compatibility applied at your country in conjunction with the principle of lawfulness established under Articles 6⁷ and 9⁸ of the GDPR, in the light of recital 50⁹ and Article 6(4) GDPR?

⁶ Article 5(1)b GDPR: Personal data shall be “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’”).

⁷ Article 6: Lawfulness of processing.

⁸ Article 9: Processing of special categories of personal data.

⁹ Recital 50 GDPR: “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

3. How do the Articles 6 and 9 of the GDPR have to be applied for the processing of special categories of personal data, in particular for scientific research ?

4. Does the duty of secrecy/medical confidentiality has any influence on the purpose limitation principle as applied in the context of scientific research ?

(Please provide information as to whether there is a reference or relationship in your national law or guidelines between the “compatible use” and the duties of secrecy/medical confidentiality?, ...)

V. Other

1. Is there any other relevant sectorial legislation in your country (e.g., on clinical trials, biobanks,) which have an interplay with the principles of purpose limitation and lawfulness as provided in the GDPR in the context of scientific research ?
2. Are there any other laws or existing documentation/guidelines, case law; case studies or discussions on national level related to the principles of purpose limitation and lawfulness as applied in the context of scientific research, and/or the secondary use of personal data in the context of scientific research, not yet mentioned above ?

No []

Yes []

If yes, please, provide your input in the table below:

Document Title and Hyperlink	Description of the relevance of this document with the topic of the research

3. Do you have any further legal sources in your country and personal views/first analysis on

- the articulation of Article 11 GDPR with the obligation to inform data subject on the re-use of data (Articles 13 & 14 GDPR), especially for medical research ?
- the articulation of Article 89(1) GDPR (obligation to de-identify data collected) and the data subjects' rights under the GDPR (including the information and access rights (articles 13 to 15) which may give the controller/processor access to the identification of data subjects ?

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”

- the application of the exemption to the information duty and appropriate measures under Article 14(5)(b) GDPR (disproportionate effects) ?

- scientific research and projects using covert and/or deceptive techniques with the transparency obligations?

4. Are you aware of any other debate in your country about the requirement of consent in the scientific research context or any other lawful ground not yet discussed or tackled above (e.g., distinctions amongst derived, between inferred data, etc;) ?

5. Please provide any additional sources you may have used for your replies which you did not yet mention:

Title of Source	Hyperlink

Thank you very much for your participation !!

ANNEX 3 – SOURCES OF INFORMATION

Legal documents

- Charter of Fundamental Rights of the European Union (OJ C 326, 26.10.2012), p. 391–407, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12012P/TXT>.
- Commission Directive 2006/17/EC of 8 February 2006 implementing Directive 2004/23/EC of the European Parliament and of the Council as regards certain technical requirements for the donation, procurement and testing of human tissues and cells (OJ L 330M , 28.11.2006, p. 162–174 (MT), OJ L 38, 9.2.2006, p. 40–52), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32006L0017>.
- Commission Directive (EU) 2015/566 of 8 April 2015 implementing Directive 2004/23/EC as regards the procedures for verifying the equivalent standards of quality and safety of imported tissues and cells (OJ L 93, 9.4.2015, p. 56–68), <https://eur-lex.europa.eu/eli/dir/2015/566/oj>.
- Council of Europe, Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine (Oviedo Convention), ETS No 164, <https://www.coe.int/en/web/bioethics/oviedo-convention>.
- Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS No 108, <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37>.
- Council of Europe, Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, ETS No. 108 +, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf.
- Council of Europe, Committee of Ministers Recommendation No. R (81) 1 on Regulations for automated medical data banks, ‘Rec(81)1’, <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804eee77>.
- Council of Europe, Recommendation CM/Rec (2019) 2 of the Committee of Ministers to member States on the protection of health-related data, https://www.apda.ad/sites/default/files/2019-03/CM_Rec%282019%292E_EN.pdf.
- Council of Europe, Recommendation No. R (97) 5 of the Committee of Ministers to member States on the protection of medical data, https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016804f0ed0.
- Council of Europe, Recommendation No. R (97) 18 of the Committee of Ministers to member States, concerning the protection of personal data collected and processed for statistical purposes, <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680508d7e>.
- Council of Europe, Recommendation Rec(2006) 4 on research on biological materials of human origin, https://www.coe.int/t/dg3/healthbioethic/Activities/10_Biobanks/Rec%282006%294%20EM%20E.pdf.
- Council of Europe, Recommendation CM/Rec (2016) 6 of the Committee of Ministers to member States on research on biological materials of human origin, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168064e900.
- 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. 31-50), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046>.
- Directive 2001/20/EC of the European Parliament and of the Council of 4 April 2001 on the approximation of the laws, regulations and administrative provisions of the Member States relating to the implementation of good clinical practice in the conduct of clinical trials on medicinal products for human use (OJ L 121, 1.5.2001, p. 34–44), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32001L0020>.
- Directive 2004/23/EC of the European Parliament and of the Council of 31 March 2004 on setting

standards of quality and safety for the donation, procurement, testing, processing, preservation, storage and distribution of human tissues and cells (OJ L 102, 7.4.2004, p. 48–58), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32004L0023>.

- Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC (OJ L 158, 27.5.2014, p. 1–76), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014R0536>.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (OJ L 119, 4.5.2016, p. 1–88), <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.

Literature

- Andersen, M.R., Storm, H.H. (on behalf of the Eurocourse Work Package 2 Group), ‘Cancer registration, public health and the reform of the European data protection framework: Abandoning or improving European public health research?’, *European Journal of Cancer*, Vol. 51, No. 9, 2015, p. 1028–1038.
- Aurucci, P., ‘Legal issues in regulating observational studies: The impact of the GDPR on Italian biomedical research’, *European Data Protection Law Review*, Vol. 5, No 2, Lexxon, 2019, pp. 197–208.
- Aymé, S., ‘Enforcement of a new data protection law in Europe: A threat and an opportunity for registries and cohorts in the field of rare diseases’, *La Revue de Médecine Interne*, Vol. 39, No. 10, p. 769–771.
- Ballantyne, A., ‘Adjusting the focus: A public health ethics approach to data research’, *Bioethics*, Vol. 33, No. 3, 2019, pp. 357–366.
- Beier, K., Lenk, C., ‘Biobanking strategies and regulative approaches in the EU: recent perspectives’, *Journal of Biorepository Science for Applied Medicine*, Vol. 3, 2015, p. 69–81.
- Bygrave, L.A., ‘The Body as Data? Biobank Regulation via the ‘Back Door’ of Data Protection Law’, *Law, Innovation and Technology*, Vol. 2, No. 1, 2010, p. 1–25.
- Chassang, G., Rial-Sebbag, E., ‘Research Biobanks and Health Databases: The WMA Declaration of Taipei, Added Value to European Legislation (Soft and Hard Law)’, *European Journal of Health Law*, Vol. 25, No. 5, Brill and Nijhoff, 2018, pp. 501–516.
- Cole, A. and Towse, A., ‘Legal Barriers to the Better Use of Health Data to Deliver Pharmaceutical Innovation’, *OHE Consulting Report*, 23 (2018), Office of Health Economic, London, 2018, <https://www.ohe.org/publications/legal-barriers-better-use-health-data-deliver-pharmaceutical-innovation>.
- Comande, G., ‘Ricerca in Sanità e Data Protection un Puzzle...Risolvibile’, rivista italiana di medicina legale e del diritto in campo sanitario, Vol. 1., 2019, p. 187–207.
- De Hert, P., Papakonstantinou, V., ‘The new general data protection regulation: Still a sound system for the protection of individuals’, *Computer Law and Security Review*, Vol. 32, No. 2, 2016, p. 179–194.
- Demotes-Mainard, J., Cornu, C., Guérin, A., ‘How the new European data protection regulation affects clinical research and recommendations’, *Therapies*, Vol. 74, No. 1, 2019.
- Djurisic, S., Rath, A., Gaber, S., Garattini, S., Bertele, V., Ngwabyt, S., Hivert, V., Neugebauer, E., Laville, M., Hiesmayr, M., Demotes-Mainard, J., Kubiak, C., Jakobsen, J., Gluud, C., ‘Barriers to the conduct of randomised clinical trials within all disease areas’, *Trials*, Vol. 18, 2017.
- Dove, E., ‘The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era’, *The Journal of Law Medicine and Ethics*, Vol. 46, No. 4, 2018, p. 1013–1030, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3240459.
- Ducato, R., ‘Data protection, scientific research, and the role of information’ (CRIDES Working Paper Series no. 1/2020), *Computar Law and Security Review*, 2020, <https://www.researchgate.net/publication/339213343>Data protection scientific research and the role of information>.
- Duguet, A., and Hervege, J., ‘Safeguards and derogations relating to processing for scientific purposes: Article 89 analysis for biobank research’, in Slokenberga, S., Tzortzatou, O., Reichel Jane

- (eds), *GDPR and Biobanking*, Springer, 2021.
- Frunză, A., Sandu, A., ‘Ethical Acceptability of Using Generic Consent for Secondary Use of Data and Biological Samples in Medical Research’, *Acta Bioethica*, Vol. 23, No. 2, 2017, p. 289-299, <https://actabioethica.uchile.cl/index.php/AB/article/view/47480/57703>.
 - Georgieva, L., and Kuner, C., ‘Article 9 Processing of special categories of personal data’, in Kuner, C., A. Bygrave, L., Docksey C., (eds.), *The EU General Data Protection Regulation (GDPR). A commentary*, Oxford University Press 2020.
 - Georgieva, L., Kuner, C., 2020
 - Georgieva, L., ‘Article 11 Processing which does not require identification’, in Kuner, C., A. Bygrave, L., Docksey C., (eds.), *The EU General Data Protection Regulation (GDPR). A commentary*, Oxford University Press 2020.
 - Georgieva, L., 2020.
 - Gola, P., ‘Article 11’, *Datenschutz-Grundverordnung: DS-GVO, VO (EU) 2016/679*, 2nd Edition, C.H. BECK, 2017.
 - Hallinan, D., ‘Broad consent under the GDPR: an optimistic perspective on a bright future’, *Life Sciences, Society and Policy*, Vol. 16, Springer, 2020.
 - Hallinan, D., *Feeding biobanks with genetic data. What role can the general data protection regulation play in the protection of genetic privacy in research biobanking in the EU?*, VUB Doctoral Thesis, Brussels, 2018.
 - Hallinan 2018
 - Hartlev, M., ‘Genomic Databases and Biobanks in Denmark’, *The Journal of Law, Medicine and Ethics*, Vol. 43, No. 4, 2015, p. 743-753.
 - Herbst, T., ‘Art. 5 Grundsätze für die Verarbeitung personenbezogener Daten’, in Kühling, J., Buchner B. (eds.), *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG*, 228, Beck, 2018.
 - Hijmans, H., Raab, C.D, ‘Ethical Dimensions of the GDPR’, in Cole, M., Boehm, F., (eds.), *Commentary on the General Data Protection Regulation*, Edward Elgar, Cheltenham, 2018 (forthcoming), <https://ssrn.com/abstract=3222677>.
 - Hintze, M., ‘Viewing the GDPR through a De-Identification Lens: A Tool for Compliance, Clarification, and Consistency’, *International Data Protection Law*, Vol. 8, No. 1, Oxford University Press, 2018, p. 86-101, <https://fpf.org/wp-content/uploads/2016/11/M-Hintze-GDPR-Through-the-De-Identification-Lens-31-Oct-2016-002.pdf>.
 - Ienca, M., Scheibner, J., Ferretti, A., Gille, F., Amann, J., Sleigh, J., Blasimme, A., Vayena, E., ‘How the General Data Protection Regulation changes the rules for scientific research’, Study for the European Parliament Panel for the Future of Science and Technology, Brussels, 2019, [http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPSTU\(2019\)634447](http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPSTU(2019)634447).
 - Ienca, M., et al., 2019.
 - Kamenjasevic, E., ‘Health data for scientific research under the CoE Recommendation and the GDPR – Part II’, Blog of KU Leuven’s Centre for IT&IP Law, 2019, <https://www.law.kuleuven.be/citip/blog/health-data-for-scientific-research-under-the-coe-recommendation-and-the-gdpr-part-ii/>.
 - Kerr, D.J., ‘Policy: EU data protection regulation - harming cancer research’, *Nature Reviews Clinical Oncology*, Vol. 11, 2014, p. 563-564.
 - Kindt, E., *Privacy and Data Protection Issues of Biometric Applications*, Springer, 2013.
 - Kostadinova, Z., ‘Purpose limitation under the GDPR: can Article 6(4) be automated?’, Tilburg University Master Thesis, <http://arno.uvt.nl/show.cgi?fid=146471>.
 - Kotschy, W., ‘Article 6 Lawfulness of processing’, in Kuner, C., A. Bygrave, L., Docksey, C., (eds.), *The EU General Data Protection Regulation (GDPR). A commentary*, Oxford University Press 2020.
 - Kramer, P., ‘Article 6, Rechtmäßigkeit der Verarbeitung’, in Auernhammer, H., Eßer, M., Kramer, P., von Lewinski, K., (eds.), *Auernhammer DSGVO/BDSG*, 5th ed., Carl Heymanns Verlag, Cologne, 2017.
 - Kuner, C., Svantesson, D.J., Cate, F.H., Lynskey, O., Millard, C., ‘The language of data privacy law (and how it differs from reality)’, *International Data Privacy Law*, Vol. 6, No. 4, 2016, p. 259-260.

- Lalova, T., et al., ‘An overview of Belgian legislation applicable to biobank research and its interplay with data protection rules’, in Slokenberga, S., Tzortzatou, O., Reichel Jane (eds), *GDPR and Biobanking*, Springer, 2021.
- Lalova, T., Negrouk, A., Deleersnijder, A., Valcke, P., Huys, I., ‘Conducting Non-COVID-19 Clinical trials during the Pandemic: Can Today’s learning Impact Framework Efficiency?’, *European Journal of Health Law*, Vol. 27, No. 5, forthcoming.
- Mészáros, J., Ho, C., ‘Big Data and Scientific Research: The Secondary Use of Personal Data under the Research Exemption in the GDPR’, *Hungarian Journal of Legal Studies*, Vol. 59, No. 4, 2018, p. 403-419.
- Minssen, T., Rajam, N., Bogers, M., ‘Clinical Trial Data Transparency and GDPR Compliance: Implications for Data Sharing and Open Innovation’, *Science and Public Policy*, 2020, p.1-11.
- Negrouk, A., Lacombe, D., ‘Does GDPR harm or benefit research participants? An EORTC point of view’, *The Lancet Oncology*, Vol. 19. No. 10, 2018, p.1278-1280.
- Negrouk, A., Lacombe, D., Meunier, F., ‘Diverging EU health regulations: The urgent need for coordination and convergence’, *Journal of Cancer Policy*, Vol. 17, 2018, p. 34-39.
- Peloquin, D., Di Maio, M., Bierer, B., ‘Disruptive and avoidable: GDPR challenges to secondary research uses of data’, *European Journal of Human Genetics*, Vol. 28, 2020, p.697-705.
- Quinn, P., ‘The Anonymisation of Research Data — A Pyrric Victory for Privacy that Should Not Be Pushed Too Hard by the eu Data Protection Framework?’, *European Journal of Health Law*, Vol. 24, No. 4, 2017, p. 347-367.
- Quinn, P., Quinn, L., ‘Big genetic data and its big data protection challenges’, *Computer Law & Security Review*, Vol. 34, No. 5, 2018, p. 1000-1018, <https://www.sciencedirect.com/science/article/abs/pii/S0267364918300827?via%3Dihub>.
- Reimer, P., ‘Artikel 5: Grundsätze für die Verarbeitung personenbezogener Daten’ in Sydow, G., (ed.), *Europäische Datenschutzgrundverordnung: Handkommentar*, Nomos, 2018, 326.
- Rial-Sebbag, E., Cambon-Thomsen, A., ‘The Emergence of Biobanks in the Legal Landscape: Towards a New Model of Governance’, *Journal of Law and Society*, Vol. 39. No. 1, 2012, p. 113-130.
- Shabani, M., Borry, P., ‘Rules for processing genetic data for research purposes in view of the new EU General Dat Protection Regulation’, *European Journal of Human Genetics*, Vol. 26, No. 2, 2018. p. 149-156.
- Spindler, G., Schmechel, P., ‘Personal Data and Encryption in the European General Data Protection Regulation’, *Journal of Intellectual Property, Information Technology and E-Commerce Law*, Vol. 7, No. 2, 2016, p. 163-177.
- de Terwagne, C., ‘Article 5 Principle relating to processing of personal data’, in Kuner, C., A. Bygrave, L., Docksey, C., (eds.), *The EU General Data Protection Regulation (GDPR). A commentary*, Oxford University Press 2020.
- De Terwagne C., Degrave É., Delforge A., & Gerard L., *La protection des données à caractère personnel en Belgique: manuel de base*, Politeia, Brussels, 2019.
- Toshkova-Nikolova, D., Feti, N., *Защита на личните данни* [Protection of personal data], ИК Труд и Право [Publishing House Trud i Pravo], 2019.
- Van Veen, E., ‘Observational health research in Europe: understanding the General Data Protection Regulation and underlying debate’, *European Journal of Cancer*, vol. 104, 2018, p. 70-80.
- Vanden Heede, E., ‘*GDPR Application in Patient Preference Studies*’, Master thesis for Intellectual Property and ICT Law under supervision of Prof. Huys, I..
- Verhenneman, G., ‘*The patient's right to privacy and autonomy against a changing healthcare model: assessing informed consent, anonymisation and purpose limitation in light of e-health and personalised healthcare*’, PhD dissertation, KU Leuven Faculty of Law, 2020.
- Verhennenman, G., 2020
- Verhenneman, G., Claes, K., Derèze, J.J., Herijgers, P., Mathieu, C., Rezda, R., Vanautgarden, M., ‘How GDPR Enhances Transparency and Fosters Pseudonymisation in Academic Medical Research’, *European Journal of Health Law*, Vol. 27(1), Brill and ‘Nijhoff, 2019, p. 40.
- Wierda, E., Eindhoven, D.C., Schalij, M.J., Borleffs, C.J.W., van Veghel, D., Michell, C.R., de Mol, B.A.J.M., Hirsch, A., Ploem., M.C., ‘Privacy of patient data in quality-of-care registries in

cardiology and cardiothoracic surgery: the impact of the new general data protection regulation EU-law’, *European Heart Journal – Quality of Care and Clinical Outcomes*, Vol. 4, No. 4, 2018, p. 239-245.

- Zuiderveen Borgesius, F., Hallinan, D., ‘Article 5’, in Boehm, F., Cole, M., (eds), *GDPR Commentary*, Elgar, 2021 (forthcoming).
- Zuiderveen Borgesius, F., Hallinan, D., 2021
- Zuiderveen Borgesius, F., ‘Singling Out People without Knowing Their Names - Behavioural targeting, pseudonymous data, and the new Data Protection Regulation’, *Computer Law & Security Review*, Vol. 32, No. 2, 2016, p. 256-271.

Case law

- ECtHR, Bărbulescu v. Romania [GC], Application No. 61496/08, 5 September 2017, CE:ECHR:2017:0905JUD006149608.
- ECtHR, I. v. Finland, Application No. 20511/03, 17 July 2008, CE:ECHR:2008:0717JUD002051103.
- ECtHR, S. and Marper v. U.K. [GC], Applications No. 30562/04 and 30566/04, 4 December 2008, CE:ECHR:2008:1204JUD003056204.
- CJEU, Judgement of 19 October 2016, Patrick Breyer v. Bundesrepublik Deutschland, C-582/14, EU:C:2016:779.
- CJEU, Judgement of 16 July 2020, Facebook Ireland and Schrems, C-311/18, EU:C:2020:559.

Other sources of information

- Article 29 Data Protection Working Party, Guidelines on consent under Regulation 2016/679, 17/EN, WP 259 rev.01, 28 November 2017, as revised on 10 April 2018, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.
- Article 29 Data Protection, Working Party, Opinion 04/2007 on the concept of personal data, 01248/07/EN, WP 136, 20 June 2007.
- Article 29 Data Protection, Working Party, Opinion 03/2013 on purpose limitation, 00569/13/EN, WP 203, 2 April 2013.
- Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 844/14/EN, WP 217, 9 April 2014.
- Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, 0829/14/EN, WP 216, 10 April 2014.
- Article 29 Data Protection Working Party, Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Systems (C-ITS), 17/EN, WP 252, 4 October 2017.
- Article 29 Data Protection Working Party, Working document on a common interpretation of Article 26(1) of Directive 5/46/EC of 24 October 1995, 2093/05/EN, WP 114, 25 November 2005.
- Council of Europe, Explanatory Report to Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, ETS No. 108 +, <https://edoc.coe.int/en/international-law/7729-convention-108-convention-for-the-protection-of-individuals-with-regard-to-the-processing-of-personal-data.html>.
- Council of Europe, Explanatory Memorandum to Recommendation No. R (97) 18 of the Committee of Ministers to member States, concerning the protection of personal data collected and processed for statistical purposes, para. 11 and 14.
- Encyclopedia of Research Design, Neil J. Salkind, N.J. (ed.), SAGE Publications, Inc., 2010, <https://sk.sagepub.com/reference/researchdesign>.
- European Commission, COM(2020) 264 final, Communication from the Commission to the European Parliament and the Council on Data protection as a pillar of citizens’ empowerment and the EU’s approach to the digital transition - two years of application of the General Data Protection Regulation.
- European Commission, DG for Health and Food Safety, *Question and Answers on the interplay*

- between the Clinical Trials Regulation and the General Data Protection Regulation, 2019,* https://ec.europa.eu/health/sites/health/files/files/documents/qa_clinicaltrials_gdpr_en.pdf.
- European Data Protection Board, Guidelines 3/2019 on processing of personal data through video devices, 10 July 2019, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.
 - European Data Protection Board, Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, 21 April 2020, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032020-processing-data-concerning-health-purpose_en.
 - European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 2 September 2020, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en.
 - European Data Protection Board, Guidelines 4/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, 21 April 2020, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/042020-use-location-data-and-contact-tracing_en.
 - European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, 4 May 2020, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en.
 - European Data Protection Board, Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR), 23 January 2019, https://edpb.europa.eu/our-work-tools/our-documents/dictamen-art-70/opinion-32019-concerning-questions-and-answers_en.
 - European Data Protection Supervisor, A Preliminary Opinion on data protection and scientific research, 6 January 2020, https://edps.europa.eu/data-protection/our-work/publications/opinions/preliminary-opinion-data-protection-and-scientific_en.
 - European Data Protection Supervisor, Guidelines concerning the processing of health data in the workplace by Community institutions and bodies, 28 September 2009, https://edps.europa.eu/data-protection/our-work/publications/guidelines/health-data-work_en.
 - European Data Protection Supervisor, Opinion 7/2015, ‘Meeting the challenges of big data, A call for transparency, user control, data protection by design and accountability’, 19 November 2015, https://edps.europa.eu/data-protection/our-work/publications/opinions/meeting-challenges-big-data_en.
 - European Medicines Agency, *Clinical Trial Regulation - Clinical Trials Information System development*, <https://www.ema.europa.eu/en/human-regulatory/research-development/clinical-trials/clinical-trial-regulation#clinical-trials-information-system-development-section>.
 - European Medicines Agency, Guideline for good clinical practice E6(R2), 1 December 2016, https://www.ema.europa.eu/en/documents/scientific-guideline/ich-e-6-r2-guideline-good-clinical-practice-step-5_en.pdf.
 - European Organisation for Research and Treatment of Cancer, *EORTC Contribution to the EMA Discussion Paper for c-Performing and Research-Supporting Infrastructures entitled “The General Data Protection Regulation: Secondary Use of Data for Medicines and Public Health Purposes Discussion Paper for Medicines Developers, Data Providers, Research-Performing and Research-Supporting Infrastructures”*, 10 July 2020, <http://www.eortc.org/app/uploads/2020/09/EMA-Secondary-use-of-health-data-Discussion-Paper-Stakeholders-consultation.pdf>.
 - Foundation Federation of Dutch Medical Scientific Societies (Federa), ‘Self-regulatory code of conduct for Observational Research with personal data (Gedragscode Gezondheidsonderzoek, 2004)’, https://www.federa.org/sites/default/files/bijlagen/coreon/code_of_conduct_for_medical_research_1.pdf.
 - Gellman, R., ‘Privacy: Finding a Balanced Approach to Consumer Options’, *Robert Gellman webpage*, 2002, <https://www.bobgellman.com/rg-docs/rg-opt-in-out-02.pdf>.
 - Gene, A., Long, W., *Webinar ‘Clinical Trials and GDPR – State of play’*, Drug Information Association (DIA), 10 July 2019.
 - Germany, Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, *Public Consultation on the theme: Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche*, 2020, p. 6-7, https://www.bfdi.bund.de/SharedDocs/Konsultationsverfahren/2020/01_Anonymisierung-

[TK.pdf? blob=publicationFile&v=6](#).

- Germany, Conference on Data Protection (*Datenschutzkonferenz*), ‘Beschluss der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung“ im Erwägungsgrund 33 der DS-GVO‘, 2019, https://www.datenschutzkonferenz-online.de/media/dskb/20190405_auslegung_bestimmte_bereiche_wiss_forschung.pdf.
- German Association for Medical Informatics, Biometry and Epidemiology (GMDS) and German Association for Data Protection and Data Security (GDD), ‘Datenschutzrechtliche Anforderungen an die medizinische Forschung unter Berücksichtigung der EU Datenschutz-Grundverordnung (DS-GVO)‘, 30, 2018, <https://www.gdd.de/arbeitskreise/datenschutz-und-datensicherheit-im-gesundheits-und-sozialwesen/materialien-und-links/datenschutzrechtliche-anforderungen-an-die-medizinische-forschung-unter-beru-cksichtigung-der-eu-datenschutz-grundverordnung/datenschutzrechtliche-anforderungen-an-die-medizinische-forschung-unter-beru-cksichtigung-der-eu-datenschutz-grundverordnung/>.
- Huys, I, ‘*Integrating patient preferences in the drug life cycle*’, Presentation for the Patient Preferences in Benefit-Risk Assessments during the Drug Life Cycle (PREFER), https://www.afmps.be/sites/default/files/content/11_prefer-fagg.pdf.
- Interview with Alexandre Entraygues, Head Data Privacy Europe at Novartis, *European Data Protection Law Review*, Vol. 5, No. 5, Lexxon, 2019.
- ISC Intelligence, ‘The Application of GDPR to Biomedical Research: Stakeholder Advisory Opinion to Assist Regulators, Prepared for the ISC Seminar on Challenges for Health Research Arising from the GDPR’, 19 November 2019, <http://www.iscintelligence.com/event.php?id=334>.
- Medical Dictionary, Definition of “Lost to follow-up”, *Medical Dictionary*, Farlex and Partners, 2009, <https://medical-dictionary.thefreedictionary.com/lost+to+follow-up>.
- Organisation for Economic Co-operation and Development, Guidelines on Human Biobanks and Genetic Research Databases, 2009, <http://www.oecd.org/sti/emerging-tech/44054609.pdf>.
- Netherlands, Ministry of Justice and Security, ‘Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet, Algemene verordening gegevensbescherming’ [Instruction manual General Data Protection Regulation and Implementating Act of the General Data Protection Regulation], 2018, <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/handleidingalgemeneverordeninggegevensbescherming.pdf>.
- Nordic Council, ‘Nordic research collaboration for better health’, <https://www.norden.org/en/information/nordic-health-co-operation>.
- Slovakia, Office for Personal Data Protection, Guidelines 2/2018, https://dataprotection.gov.sk/uouu/sites/default/files/zakonnost_aktualizovana_verzia_22.01.2019.pdf.
- Southerington, T., ‘GA4GH GDPR Brief: The Finnish Secondary Use Act 2019 (May 2020 Bonus Brief)’ [blog post], 21 May 2020, <https://www.ga4gh.org/news/ga4gh-gdpr-brief-the-finnish-secondary-use-act-2019-may-2020-bonus-brief/>.
- UK Information Commissioner’s Office, Overview ‘*Lawful Basis for Processing*’, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/>.
- UK Medical Research Council, ‘GDPR: Answers to some frequently asked questions (FAQs) - Can I share data with colleagues now that GDPR is in force?’, <http://www.highlights.rsc.mrc.ac.uk/GDPR/share.html>.
- UK Medical Research Council, ‘*Guidance Note 3, General Data Protection Regulation (GDPR): Consent in Research and Confidentiality*’, March 2018, as updated in March 2019, <https://mrc.ukri.org/research/facilities-and-resources-for-researchers/regulatory-support-centre/gdpr-resources/>.
- UK Health Research Authority, ‘Safeguards’ [webpage], last updated in 2018, <https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-detailed-guidance/safeguards/>.
- UK Health Research Authority, ‘Transparency’ [webpage], last updated in 2018, <https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-detailed-guidance/transparency/>.
- UK Secretary of State for Health and Social Care, Decision ‘*Coronavirus (COVID-19): notice under*

regulation 3(4) of the Health Service (Control of Patient Information) Regulations 2002 – general, 29 July 2020, <https://www.gov.uk/government/publications/coronavirus-covid-19-notification-of-data-controllers-to-share-information/coronavirus-covid-19-notice-under-regulation-34-of-the-health-service-control-of-patient-information-regulations-2002-general>.

- World Health Organisation, Operational guidelines for Ethics Committees that review biomedical research, Geneva, 2000, <https://www.who.int/tdr/publications/documents/ethics.pdf>.
- World Medical Association, Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Subjects, June 1964, <https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/>.
- Declaration of Helsinki
- World Medical Association, ‘Declaration of Taipei - Research on Health Databases, Big Data and Biobanks’, October 2002, <https://www.wma.net/policies-post/wma-declaration-of-taipei-on-ethical-considerations-regarding-health-databases-and-biobanks/>.
- Declaration of Taipei
- World Medical Association, ‘International Code of Medical Ethics’, 1949, last amended in 2006, <https://www.wma.net/policies-post/wma-international-code-of-medical-ethics/>.

National sources of information

Member State	National legislation	Case-law	Other documents
Belgium	<ul style="list-style-type: none"> ▪ Belgian Law on the processing of personal data of 30 July 2018 (<i>Wet betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens</i>); ▪ Law of 7 May 2004 “<i>Wet inzake experimenten op de menselijke persoon</i>”, available at: https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2004050732&table_name=wet; ▪ Biobank Act ▪ Act of 19 December 2008 on Human Body Material (<i>Loi relative à l'obtention et à l'utilisation de matériel corporel humain destiné à des applications médicales humaines ou à des fins de recherche scientifique</i>), available at: http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2008121944&table_name=loi) ▪ Law of 22 August 2002 on Patient Rights 		<ul style="list-style-type: none"> ▪ Van Gyseghem J.-M. (2018). “Les catégories particulières de données à caractère personnel” in Le règlement général sur la protection des données (RGPD/GDPR), Larcier ▪ Terwagne C., Degrave É., Delforge A., & Gerard L. (2019). <i>La protection des données à caractère personnel en Belgique: manuel de base</i>. Politeia, p. 124-130.
Bulgaria	<ul style="list-style-type: none"> ▪ Personal Data Protection Act (PDPA), available in English at: https://www.cpdp.bg/en/index.php?p=element&aid=1194; 		<ul style="list-style-type: none"> ▪ Desislava Toshkova-Nikolova, Nevin Feti, “Заштита на личните данни” [Protection of personal data], ИК Труд и Право

Member State	National legislation	Case-law	Other documents
	<ul style="list-style-type: none"> ▪ Promotion of Scientific Research Act, available at https://www.lex.bg/laws/lde/c/2135472978; ▪ The Health Act (2004); ▪ The Protection against Discrimination Act (2003); ▪ The Law on Transplantation of Organs, Tissues and Cells (2004) ▪ Code of Professional Ethics of Medical Doctors ▪ Higher Education Act 		[Publishing House Trud i Pravo] (2019)
Croatia			
Cyprus			
Denmark	<ul style="list-style-type: none"> ▪ Act No. 502 of 23 May 2018 on supplementary provisions to the regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. 		
Estonia	<ul style="list-style-type: none"> ▪ Estonian Personal Data Protection Act Implementation Act, available in English at: https://www.riigiteataja.ee/en/eli/523012019001/consolidate 		
Finland	<ul style="list-style-type: none"> ▪ Act on Secondary Use of Health and Social Data (552/2019), available at: https://stm.fi/en/secondary-use-of-health-and-social-data; ▪ Data Protection Act, available at: https://www.finlex.fi/en/laki/kaannokset/2018/en20181050.pdf 	<ul style="list-style-type: none"> ▪ FinData, available at: https://www.findata.fi/en/; ▪ T. Southerington, 'GA4GH GDPR Brief: The Finnish Secondary Use Act 2019', 21.5.2020, available at: https://www.ga4gh.org/news/ga4gh-gdpr-brief-the-finnish-secondary-use-act-2019-may-2020-bonus-brief/ 	
France	<ul style="list-style-type: none"> ▪ Civil Code ▪ French data protection act (<i>Loi Informatique et Libertés – LIL</i>); ▪ <i>Code de la Santé Publique (PHC)</i>; ▪ Code of Research, available at: https://www.legifrance.gouv.fr/codes/id/LEGIARTI000027747800/2013-07-24/ 		<ul style="list-style-type: none"> ▪ Bill of bioethics law, projet de loi n°2658
Germany	<ul style="list-style-type: none"> ▪ National data protection act (BDSG); ▪ Medicinal Product Law 	<ul style="list-style-type: none"> ▪ Judgement of the German Federal Constitutional Court 	<ul style="list-style-type: none"> ▪ <i>Musterberufsordnung für Ärzte 2015</i> – the

Member State	National legislation	Case-law	Other documents
		<ul style="list-style-type: none"> <li data-bbox="382 256 1065 804">▪ <i>(Bundesverfassungsgericht – BVerfGE)</i> BVerfGE 35, 79, 112, available at: https://dejure.org/diense/vernetzung/rechtsprechung?Gericht=BVerfG&Datum=01.03.1978&Aktenzeichen=1%20BvR%20333/75; <li data-bbox="755 563 1065 804">▪ BVerfGE 47, 327, 367, available at: https://dejure.org/diense/vernetzung/rechtsprechung?Gericht=BVerfG&Datum=29.05.1973&Aktenzeichen=1%20BvR%20424%2F71. 	<ul style="list-style-type: none"> <li data-bbox="1097 256 1395 923">▪ Code of Conduct for Doctors; Datenschutzkonferenz, <i>Beschluss der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung“ im Erwägungsgrund 33 der DS-GVO (2019)</i>, available at: https://www.datenschutzkonferenz-online.de/media/dskb/20190405_auslegung_bestimmte_bereiche_wissenschaft_forschung.pdf <li data-bbox="1097 923 1395 1828">▪ <i>GMDS and GDD, Datenschutzrechtliche Anforderungen an die medizinische Forschung unter Berücksichtigung der EU Datenschutz-Grundverordnung (DS-GVO), (2018)</i>, 30, available at: https://www.gdd.de/arbeitskreise/datenschutz-und-datosicherheit-im-gesundheits-und-sozialwesen/materialien-und-links/datenschutzrechtl_iche-anforderungen_an-die-medizinische-forschung-unter-beruksichtigung-der-eu-datenschutz-grundverordnung/date_nschutzrechtl_iche-anforderungen-an-die-medizinische-forschung-unter-beruksichtigung-der-eu-datenschutz-grundverordnung/
Greece	<ul style="list-style-type: none"> <li data-bbox="382 1828 747 2005">▪ Law 4310/2014 on Research & Innovation, available at: https://www.kodiko.gr/nomologia/document_navigation/100926/nomos-4310-2014; 		<ul style="list-style-type: none"> <li data-bbox="1097 1828 1395 2028">▪ EXPLANATORY MEMORANDUM to the Draft Law “Hellenic Data Protection Authority, Implementation

Member State	National legislation	Case-law	Other documents
	<ul style="list-style-type: none"> ▪ Law 4386/2016 on Rules of Research, available at: https://www.kodiko.gr/nomologia/document_navigation/197924/nomos-4386-2016. ▪ Law 4624/2019, Official Government Gazette A' 137/29.08.2019, http://www.et.gr/idocs-nph/search/pdfViewerForm.html?args=5C7QrtC22wFqnM3eAbJzrXdtvSoClrL8WkQtR1OJjJd5MXD0LzQTLWPU9yLzB8V68knBzLCmTXKaO6fpVZ6Lx9hLslJUqeIQFO1o1b-ZCxkj8oDGZfpPVRON0QvoraqawUQAqlqKetE. 		<p>Measures of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and Transposition into National Legislation of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016";</p> <ul style="list-style-type: none"> ▪ Hellenic Data Protection Authority, 'Opinion No. 1/2020.'
Hungary	<ul style="list-style-type: none"> ▪ 2019 CXXIII. Act amending the LXXVI of 2014 Act and certain related legal provisions on Scientific Research, Development and Innovation – 2019, available at: https://mkogy.jogtar.hu/jogs_zabaly?docid=A1900123.T_V 		
Italy	<ul style="list-style-type: none"> ▪ Italian data protection act (PDPC) ▪ Data Protection Code (PDPC), available in English at: https://www.garanteprivacy.it/documents/10160/0/Data+Protection+Code.pdf/7f4dc718-98e4-1af5-fb44-16a313f4e70f?version=1.3; ▪ Legislative decree no 101 of 10 August 2018 	<ul style="list-style-type: none"> ▪ G. Comandé, Ricerca in sanità e data protection un puzzle ... Risolvibile, Anno XLI 1 RIV. IT. DI MED. LEG. (2019); ▪ 2014 Medical Deontological rules ▪ Garante, <i>Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101 [9124510]</i>, available at: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9124510 	
Latvia	<ul style="list-style-type: none"> ▪ Latvian Data Protection Law (PDPL), available at: https://likumi.lv/ta/id/300099#p-32.; 		

Member State	National legislation	Case-law	Other documents
The Netherlands	<ul style="list-style-type: none"> ▪ The Law on Patients' Right, available at: https://likumi.lv/ta/en/en/id/203008-law-on-the-rights-of-patients. 		<ul style="list-style-type: none"> ▪ Foundation Federation of Dutch Medical Scientific Societies (Federa): Self-regulatory code of conduct for Observational Research with personal data (Gedragscode Gezondheidsonderzoek, 2004), available at https://www.federa.org/sites/default/files/bijlagen/coreon/code_of_conduct_for_medical_research_1.pdf. ▪ Autoriteit Persoonsgegevens, Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming, 2018, 41, available at: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/handleidingalgemenerverordeninggegevensbescherming.pdf
Portugal	<ul style="list-style-type: none"> ▪ Law No. 58/2019 		
Romania	<ul style="list-style-type: none"> ▪ Governmental Ordinance No. 57/2002, available at: http://www.cdep.ro/pls/legis/legis_pck.htm_act_text?id=37578; ▪ Law on health reform ▪ Law No. 190/2018 on implementing measures of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, available at: https://lege5.ro/Gratuit/gi4d_snjugi2q/legea-nr-190-2018-privind-masuri-de-punere-in-aplicare-a-regulamentului-ue-2016-679-al-parlamentului-european-si-al-consiliului-din-27-aprilie-2016-privind- 		<ul style="list-style-type: none"> ▪ Decree of the Ministry of Health No. 904/25.07.2006, available at http://www.scumc.ro/LegisDir/42.%20Ordin%20904%20din%202006.pdf ▪ Frunză, A., and Sandu, A. (2017), Ethical acceptability of using generic consent for secondary use of data and biological samples in medical research. Acta Bioethica, 23(2), available at https://actabioethica.ucfile.cl/index.php/ABA/article/view/47480/57703

Member State	National legislation	Case-law	Other documents
	<p><u>protectia-persoanelor-fizice-in-ceea-ce-priv;</u></p> <ul style="list-style-type: none"> ▪ Law No. 95/2006 on health care reform (<i>Legea nr. 95/2006 privind reforma în domeniul sănătății</i>), 1 May 2006, available at: https://lege5.ro/App/Document/g42tmnjsg/legea-nr-95-2006-privind-reforma-in-domeniul-sanatatii?d=22.04.2020&forma=zi 		
Slovakia	<ul style="list-style-type: none"> ▪ Data Protection Act, available at: https://www.zakonypreludisk/zz/2018-18 		<ul style="list-style-type: none"> ▪ National guidelines, available at: https://dataprotection.gov.sk/uouu/sites/default/files/zakonnost_aktualizovana_verzia_22.01.2019.pdf
Slovenia	<ul style="list-style-type: none"> ▪ 2004 Personal Data Protection Act (<i>ZVOP-1</i>); ▪ Proposal for the new Personal Data Protection Act (<i>ZVOP-2</i>); ▪ Research and Development Activities Act, available at: http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO3387 		
Norway	<ul style="list-style-type: none"> ▪ Health Research Act (<i>Lov om medisinsk og helsefaglig forskning</i>), available at: https://lovdata.no/dokument/NL/lov/2008-06-20-44 		<ul style="list-style-type: none"> ▪ Department Guidelines on medical and health research (<i>Veileder til lov 20. juni 2008 nr. 44 om medisinsk og helsefaglig forskning</i>)
United Kingdom	<ul style="list-style-type: none"> ▪ UK Data Protection Act 2018 		<ul style="list-style-type: none"> ▪ ICO, ‘Lawful Basis for Processing’, available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/; ▪ Department of Health and Social Care, Covid-19 – Notice under Regulation 3(4) of the Health Service Control of Patient Information Regulations 2002, March 20, 2020; ▪ Health Research Authority,

Member State	National legislation	Case-law	Other documents
			<p>'Transparency' (Health Research Authority), available at: https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-detailed-guidance/transparency</p>

ANNEX 4 - ACRONYMS AND ABBREVIATIONS

Acronyms and Abbreviations	Meaning
BBMRI-ERIC	Biobanking and BioMolecular Resources Research Infrastructure – European Research Infrastructure Consortium
Charter	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
CNIL	French SA (<i>Commission nationale de l'informatique et des libertés</i>)
CoE	Council of Europe
CT	Clinical trials
CTC	Clinical Trial College
CTD	Clinical Trials Directive (EC) 2001/20/EC
CTR	Clinical Trials Regulation (EU) 536/2014
DH	Declaration of Helsinki
DPA	Slovakian Data Protection Act
DPO	Data Protection Officer
DRD	Data Retention Directive
DT	Declaration of Taipei
EC(s)	Ethics committee(s)
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EEA	European Economic Area
EFTA	European Free Trade Association
EMA	European Medicines Agency
EORTC	European Organisation for Research and Treatment of Cancer
EU	European Union
GCP	Good Clinical Practice
GDD	The German Association for Data Protection and Data Security
GDPR	General Data Protection Regulation
GMDS	German Association for Medical Informatics, Biometry and Epidemiology
HBGRD Guidelines	Guidelines for Human Biobanks and Genetic Research databases
IC	Informed consent
ICH	International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use
ICO	Information Commissioner's Office (UK SA)
LIL	French data protection law (<i>Loi Informatique et Libertés</i>)
MS(s)	Member State(s)
OSS mechanism	One-stop-shop mechanism
PDPA	Bulgarian Personal Data Protection Act
PHC	French <i>Code de la Santé Publique</i>
PDPC	Italian data protection act
Rec	Recommendation
REC	French <i>Comité de Protection des Personnes</i>

Acronyms and Abbreviations	Meaning
RIHP	Researches Involving Human Persons
SA(s)	Supervisory Authority(-ies)
STOA	European Parliament Panel for the Future of Science and Technology
TFEU	Treaty on the Functioning of the European Union
UK	United Kingdom
WMA	World Medical Association
WP29	Working Party 29

ANNEX 5 - ENDNOTES

¹ For the purposes of this report, we use uniformly ‘secondary use’ understood as ‘re-use of personal data for a new purpose’, but we acknowledge that the GDPR employs the term ‘further processing’. See also the discussion in Section 4.2.2.2 on primary versus secondary use of personal data.

² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (OJ L 119, 4.5.2016, p. 1-88).

³ In this report, the term ‘health data’ is used to mean ‘data concerning health’ rather than ‘medical data’ the latter having a more narrow scope. On these concepts, see EDPS, Guidelines concerning the processing of health data in the workplace by Community institutions and bodies, 28 September 2009.

⁴ This question raises precisely because the GDPR contains specific principles, provisions, and possibilities of derogations for scientific research.

⁵ This priority was mentioned in European Commission, COM(2020) 264 final, Communication from the Commission to the European Parliament and the Council on Data protection as a pillar of citizens’ empowerment and the EU’s approach to the digital transition - two years of application of the General Data Protection Regulation, p. 2. This does not mean however that this topic is not discussed herein: e.g., see the new Finnish Act on the Secondary Use of Health and Social Data (552/2019), which entered into force on May 1, 2019, available at the Finnish Ministry of Social Affairs and Health, Secondary use of health and social data, available at: <https://stm.fi/en/secondary-use-of-health-and-social-data>, which regulates re-use of personal data in public databases for described purposes, such as knowledge management.

⁶ See e.g. examples from Estonia (Section 5.2.2) and Finland (Section 5.3.4).

⁷ This distinction was affirmed by the EDPB in European Data Protection Board, Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR), 23 January 2019.

⁸ See Verhenneman, G., ‘*The patient's right to privacy and autonomy against a changing healthcare model: assessing informed consent, anonymisation and purpose limitation in light of e-health and personalised healthcare*’, PhD dissertation, KU Leuven Faculty of Law, 2020, p. 206 and 224.

⁹ We focused on several key documents, however other conventions and recommendations of special importance must also be mentioned, in particular Council of Europe, Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine (Oviedo Convention), ETS No 164, and its Additional protocol on Biomedical Research (2005) and Council of Europe, Recommendation No R (97) 18 of the Committee of Ministers to member States, concerning the protection of personal data collected and processed for statistical purposes.

¹⁰ Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS No 108.

¹¹ Council of Europe, Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, ETS No. 108 +.

¹² Convention 108 has been ratified by 55 countries and amongst them nine countries are not member of the CoE. Convention 108+ adopted in 2018 has in the meantime been signed by 42 countries and ratified by eight of them.

¹³ Council of Europe, Explanatory Report to Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, ETS No. 108 +, p. 20, n°43.

¹⁴ *Id.* See also Council of Europe, Explanatory Memorandum to Recommendation No. R (97) 18 of the Committee of Ministers to member States, concerning the protection of personal data collected and processed for statistical purposes, para. 11 and 14.

¹⁵ Council of Europe, Recommendation No R (97) 18.

¹⁶ Council of Europe, Explanatory Memorandum to Recommendation No. R (97) 18, paragraph 14.

¹⁷ Council of Europe, Explanatory Memorandum to Recommendation No. R (97) 18, paragraph 4.

¹⁸ Convention 108+ slightly changed the wording of Article 5.

¹⁹ Council of Europe, Committee of Ministers Recommendation No. R (81) 1 on Regulations for automated medical data banks, (‘Rec(81)1’ or ‘CoE, Rec(81)1’).

²⁰ Article 5(4) of CoE Recommendation (81) 1 states: “*Without the data subject's express and informed consent, the existence and content of his medical record may not be communicated to persons or bodies outside the fields of medical care, public health or medical research, unless such a communication is permitted by the rules on medical professional secrecy.*”

²¹ Article 5(4) of CoE Recommendation (81) 1.

²² Council of Europe, Recommendation No. R (97) 5 of the Committee of Ministers to member States on the protection of medical data.

²³ See Section 12(2), which points to these legal bases for use of medical data for scientific research, if not anonymous, as secondary purpose.

²⁴ Clearly, a need was felt to distinguish scientific research by the treating physician from scientific research by others. A possible explanation may be that this is an indication for what, at that time, were considered reasonable expectations from the data subjects as compatible use and purposes. By allowing the further use of data by the treating physician on the condition that the data subject was informed and had the possibility to opt-out, it was encoded in law that this was considered standard practice and not interfering in the relationship of trust between the treating physician and the patient, and provided as such a

legal basis. Apparently, one felt that the same assumption could not be made when the data were shared with others since for this scenario additional safeguards were included.

²⁵ Both the profession of healthcare practitioner and of researcher has changed since in both professions multidisciplinary teamwork has become increasingly important.

²⁶ Council of Europe, Recommendation CM/Rec (2019)2 of the Committee of Ministers to member States on the protection of health-related data. Verhenneman notes that “it was in particular due to the promulgation of the GDPR that the Council of Europe needed to review its 1997 Recommendations, as well as Convention 108. See Verhenneman 2020, p. 253.

²⁷ Council of Europe, Recommendation CM/Rec (2016)6 of the Committee of Ministers to member States on research on biological materials of human origin, which is a successor of Council of Europe, Recommendation Rec(2006)4 on research on biological materials of human origin.

²⁸ See Preamble of CoE Recommendation CM/Rec(2016)6

²⁹ World Medical Association, Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Subjects, June 1964.

³⁰ See Preamble of the Declaration of Helsinki.

³¹ The interests of and respect for the individual are the cornerstones, as well as the right to self-determination and right of the individual to make informed decisions in relation to research. (Articles 8, 9 and 26 Declaration of Helsinki). Medical research is also required to meet certain standards of quality and publicity (Articles 21-22 Declaration of Helsinki).

³² Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC (OJ L 158, 27.5.2014, p. 1–76).

³³ Article 6 of the Declaration of Helsinki: “[...] to understand the causes, development and effects of diseases and improve preventive, diagnostic and therapeutic interventions (methods, procedures and treatments). Even the best proven interventions must be evaluated continually through research for their safety, effectiveness, efficiency, accessibility and quality”.

³⁴ One could also ask whether the GDPR rules on consent will have an influence on the interpretation of consent under e.g., the Declaration of Helsinki.

³⁵ World Medical Association, Declaration of Taipei - Research on Health Databases, Big Data and Biobanks, October 2002.

³⁶ See Preamble of the Declaration of Taipei: “**in concordance with the Declaration of Helsinki, it provides additional ethical principles for their use in Health Databases and Biobanks**”.

³⁷ Furthermore, it has been noted that the focus on biobanks echoes recent changes to national approaches with the adoption of so-called “Biobank Acts” (Sweden, Finland, Belgium), see Chassang, G., Rial-Sebbag, E., ‘Research Biobanks and Health Databases: The WMA Declaration of Taipei, Added Value to European Legislation (Soft and Hard Law)’, *European Journal of Health Law*, Vol. 25, No. 5, Brill and Nijhoff , 2018, pp. 501-516.

³⁸ Declaration of Taipei, Preamble, Paragraph 4.

³⁹ Declaration of Taipei, Ethical principles, Paragraph 12.

⁴⁰ Ballantyne, A., ‘Adjusting the focus: A public health ethics approach to data research’, *Bioethics*, Vol. 33, No. 3, 2019, pp. 357-366.

⁴¹ *Id.*

⁴² *Id.*

⁴³ Organisation for Economic Co-operation and Development, Guidelines on Human Biobanks and Genetic Research Databases, 2009. The guidelines are not legally binding..

⁴⁴ See also Duguet, A., and Herve, J., ‘Safeguards and derogations relating to processing for scientific purposes: Article 89 analysis for biobank research’, in Slokenberga, S., Tzortzatou, O., Reichel Jane (eds), *GDPR and Biobanking*, Springer, 2021. According to Duguet and Herve, the OECD “gives priority to facilitating research with biobanks, while the rights of the subjects involved are secondary and in accordance with national legislation”.

⁴⁵ Act of 19 December 2008 regarding the procurement and use of human bodily material destined for human medical applications or for scientific research.

⁴⁶ See e.g. the example of how the view on multi-disciplinary research has changed in the new CoE Recommendation CM/Rec (2019)2 in comparison to CoE Recommendation No. R (97) 5.

⁴⁷ If the EDPA would dispose of such documents, we might be able to analyse them. So far, we went through the various documents accessible on <https://eur-lex.europa.eu/legal-content/FR/HIS/?uri=CELEX:32016R0679&qid=1597043984880>.

⁴⁸ Article 29 Data Protection Working Party, Guidelines on consent under Regulation 2016/679, 17/EN, WP 259 rev.01, 28 November 2017, as revised on 10 April 2018. This reference has been mentioned in European Data Protection Board, Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, 21 April 2020.

⁴⁹ European Data Protection Supervisor, A Preliminary Opinion on data protection and scientific research, 6 January 2020, p. 12.

⁵⁰ Recital 157 of the GDPR.

⁵¹ Belgium, Bulgaria, Croatia, Cyprus, France, Germany, Greece, Italy, Latvia, the Netherlands, Romania, Slovakia, Slovenia and Norway.

⁵² BVerfGE 35, 79, 112 f.; BVerfGE 47, 327, 367, available at <https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=BVerfG&Datum=01.03.1978&Aktenzeichen=1%20BvR%2033%2F75> and <https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=BVerfG&Datum=29.05.1973&Aktenzeichen=1%20BvR%2042%2F71>.

⁵³ No answer for Denmark.

⁵⁴ Foundation Federation of Dutch Medical Scientific Societies (Federa), ‘Self-regulatory code of conduct for Observational Research with personal data (Gedragscode Gezondheidsonderzoek, 2004)’.

⁵⁵ See sec. 2 of the Finnish Act on the Secondary Use of Health and Social Data. See also below.

⁵⁶ Regulation (EU) No 536/2014 (Clinical Trials Regulation) is expected to come into application in 2022. The timing depends on confirmation of full functionality of the Clinical Trials Information System (CTIS) through an independent audit (scheduled to commence in December 2020), and Clinical Trials Regulation will become applicable six months after the European Commission publishes notice of this confirmation. For more information, see European Medicines Agency, *Clinical Trial Regulation - Clinical Trials Information System development*. The term of investigator is used to designate the responsible individual for the conduct of a CT at a clinical trial site (Article 2(15)), while sponsor is the individual, company, institution or organisation which takes responsibility for the initiation, for the management and for setting up the financing of the clinical trials (Article 2(14)). Recital 81 also refers to ‘non-commercial sponsors’, relying on funding ‘which comes partly or entirely from public funds or charities’ and the need to stimulate their research.

⁵⁷ See Article 28(1)(c) and Articles 28-32 Clinical Trials Regulation.

⁵⁸ Recital 29 and Article 28(2) al. 2 Clinical Trials Regulation.

⁵⁹ EDPB Opinion 3/2019; European Commission, DG for Health and Food Safety, *Question and Answers on the interplay between the Clinical Trials Regulation and the General Data Protection Regulation*, 2019.

⁶⁰ These are in particular regarding the choice of legal basis, the distinction between consent for participation in research and consent as one of the lawful grounds for processing of data, and the differentiation between primary and secondary use of clinical trial data. This occupies a prominent part of the scholarly debate. See e.g. Van Veen, E., ‘Observational health research in Europe: understanding the General Data Protection Regulation and underlying debate’, *European Journal of Cancer*, vol. 104, 2018, p. 70-80; Negrouk, A., Lacombe, D., ‘Does GDPR harm or benefit research participants? An EORTC point of view’, *The Lancet Oncology*, Vol. 19, No. 10, 2018, p.1278-1280; Demotes-Mainard, J., Cornu, C., Guérin, A., ‘How the new European data protection regulation affects clinical research and recommendations’, *Therapies*, Vol. 74, No. 1, 2019; Ienca, M., Scheibner, J., Ferretti, A., Gille, F., Amann, J., Sleigh, J., Blasimme, A., Vayena, E., ‘How the General Data Protection Regulation changes the rules for scientific research’, Study for the European Parliament Panel for the Future of Science and Technology, Brussels, 2019; Minssen, T., Rajam, N., Bogers, M., ‘Clinical Trial Data Transparency and GDPR Compliance: Implications for Data Sharing and Open Innovation’, *Science and Public Policy*, 2020, p.1-11.

⁶¹ In the research community, however, there is still uncertainty as to how to comply with these two pieces of legislation, especially when it comes to secondary use of personal data. See e.g. Peloquin, D., Di Maio, M., Bierer, B., ‘Disruptive and avoidable: GDPR challenges to secondary research uses of data’, *European Journal of Human Genetics*, Vol. 28, 2020, p.697-705; Aymé, S., ‘Enforcement of a new data protection law in Europe: A threat and an opportunity for registries and cohorts in the field of rare diseases’, *La Revue de Médecine Interne*, Vol. 39, No. 10, 2018, p. 769-771; Wierda, E., Eindhoven, D.C., Schalij, M.J., Borleffs, C.J.W., van Veghel, D., Michell, C.R., de Mol, B.A.J.M., Hirsch, A., Ploem, M.C., ‘Privacy of patient data in quality-of-care registries in cardiology and cardiothoracic surgery: the impact of the new general data protection regulation EU-law’, *European Heart Journal – Quality of Care and Clinical Outcomes*, Vol. 4, No. 4, 2018, p. 239-245; Kerr, D.J., ‘Policy: EU data protection regulation - harming cancer research’, *Nature Reviews Clinical Oncology*, Vol. 11, 2014, p. 563-564; Andersen, M.R., Storm, H.H. (on behalf of the Eurocourse Work Package 2 Group), ‘Cancer registration, public health and the reform of the European data protection framework: Abandoning or improving European public health research?’, *European Journal of Cancer*, Vol. 51, No. 9, 2015, p. 1028-1038.

⁶² EDPS, A Preliminary Opinion on data protection and scientific research, p. 35.

⁶³ See e.g. the overview of discrepancies in EMA’s and other national regulatory body’s responses to the COVID-19 pandemic, as summarized in Lalova, T., Negrouk, A., Deleersnijder, A., Valcke, P., Huys, I., ‘Conducting Non-COVID-19 Clinical trials during the Pandemic: Can Today’s learning Impact Framework Efficiency?’, *European Journal of Health Law*, Vol. 27, No. 5, forthcoming.

⁶⁴ Due to the soon-to-be-applicable Clinical Trials Regulation. However, it must be noted that even the Clinical Trials Regulation does not equal full harmonization, see e.g., Negrouk, A., Lacombe, D., Meunier, F., ‘Diverging EU health regulations: The urgent need for co ordination and convergence’, *Journal of Cancer Policy*, Vol. 17, 2018, p. 34-39; and Djuricic, S., Rath, A., Gaber, S., Garattini, S., Bertele, V., Ngwabyt, S., Hivert, V., Neugebauer, E., Laville, M., Hiesmayr, M., Demotes-Mainard, J., Kubiak, C., Jakobsen, J., Gluud, C., ‘Barriers to the conduct of randomised clinical trials within all disease areas’, *Trials*, Vol. 18, 2017.

⁶⁵ Beier, K., Lenk, C., ‘Biobanking strategies and regulative approaches in the EU: recent perspectives’, *Journal of Biorepository Science for Applied Medicine*, Vol. 3, 2015, p. 69-81.

⁶⁶ Id. at 77. In the interest of completeness, it must be noted that according to Rial-Sebag and Cambon-Thomsen, the general approaches to biobank regulation are two: countries where specific legislation has been adopted, and countries where provisions with regard to biobanks have been integrated into wider legislative provisions, see Rial-Sebag, E., Cambon-Thomsen, A., ‘The Emergence of Biobanks in the Legal Landscape: Towards a New Model of Governance’, *Journal of Law and Society*, Vol. 39, No. 1, 2012, p. 113-130.

⁶⁷ The Act of 19 December 2008 on Human Body Material (*Loi relative à l'obtention et à l'utilisation de matériel corporel humain destiné à des applications médicales humaines ou à des fins de recherche scientifique*, available at: http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2008121944&table_name=loi) For an overview of the interplay between the Belgian biobank law and data protection legislation, see Lalova, T., et al., ‘An overview of Belgian legislation applicable to biobank research and its interplay with data protection rules’, in Slokenberga, S., Tzortzatou, O., Reichel Jane (eds), *GDPR and Biobanking*, Springer, 2021.

⁶⁸ Until recently, biobanks in Denmark were governed by a complex and rather unique system construed by data protection legislation, ethics review, and legal rules pertaining to patients’ rights, see Hartlev, M., ‘Genomic Databases and Biobanks in Denmark’, *The Journal of Law, Medicine and Ethics*, Vol. 43, No. 4, 2015, p. 743-753.

⁶⁹ In Bulgaria, a patchwork of provisions applies to biobanking in Bulgaria: Art. 141-144 (concerning genetic laboratories) of the Health Act (2004), the Protection against Discrimination Act (2003), the Law on Transplantation of Organs, Tissues and Cells (2004), from which scope the use of organs for research purposes is excluded (Article 1), a number of Ordinances that

further implement the Law on Transplantation, general administrative and civil law provisions (concerning biobank custodianship) and finally, the ethical framework (soft-law).

⁷⁰ Directive 2004/23/EC of the European Parliament and of the Council of 31 March 2004 on setting standards of quality and safety for the donation, procurement, testing, processing, preservation, storage and distribution of human tissues and cells (OJ L 102, 7.4.2004, p. 48–58); Commission Directive 2006/17/EC of 8 February 2006 implementing Directive 2004/23/EC of the European Parliament and of the Council as regards certain technical requirements for the donation, procurement and testing of human tissues and cells (OJ L 330M , 28.11.2006, p. 162–174 (MT), OJ L 38, 9.2.2006, p. 40–52); and Commission Directive (EU) 2015/566 of 8 April 2015 implementing Directive 2004/23/EC as regards the procedures for verifying the equivalent standards of quality and safety of imported tissues and cells (OJ L 93, 9.4.2015, p. 56–68).

⁷¹ Ienca, M., et al., 2019.

⁷² Article 1 of Directive 2004/23/EC.

⁷³ See e.g. the Belgian Act on Human Body Material (19 December 2008) which is intended, inter alia, to implement the Directives, but which also includes scientific research purposes in its scope.

⁷⁴ Articles 41-43 Clinical Trials Regulation.

⁷⁵ Articles 77-79 Clinical Trials Regulation.

⁷⁶ EDPB Opinion 3/2019, p. 4, European Commission, DG for Health and Food Safety, *Question and Answers on the interplay between the Clinical Trials Regulation and the General Data Protection Regulation*, Question 3.

⁷⁷ See EDPB Guidelines 03/2020, p. 7. It must be noted that these guidelines make a specific reference to the first two legal bases, because they were considered the most suitable in relation to primary uses of data concerning health in the COVID-19 context.

⁷⁸ We should regret that some guidelines has put forward that, when processing special categories of data, the data controller must combine Articles 6 and 9. This does not look compliant with the economy of the GDPR that makes a clear distinction between the ‘normal’ data and the ones from special categories. Requesting that the controller must find a lawful base in Article 6 and then in Article 9 is a not adequate. GDPR sets two categories of data with lawful grounds each. This is obvious when we compare the various grounds which are crossing each other’s. This shows they do not need to be overlaid. It is one article or the other. The only reason to overlay the two articles may lie in the fact that Article 2(i) provides for the right to affix the stamp only for processing operations carried out on the basis of Article 6(1)(e) or (f). But can we legally twist the principles of the GDPR to correct a legislative error. Instead, it would be preferable to alert the legislature to fix this error as it has done since 2016.

⁷⁹ Recital 27 Clinical Trials Regulation.

⁸⁰ EDPB Opinion 3/2019, p. 5, European Commission, DG for Health and Food Safety, Question and Answers on the interplay between the Clinical Trials Regulation and the General Data Protection Regulation, Question 4. The EDPS also asserted the logic shared by EDPB and the Commission but further acknowledged that the conditions under which IC for participation in research might be deemed an appropriate safeguard are still unclear: EDPS, A Preliminary Opinion on data protection and scientific research, p. 19. Moreover, the EDPS concluded that the notion of consent in the two areas requires further discussion between the research community and data protection experts.

⁸¹ *Id.* at 19.

⁸² Article 8, 22 Aout 2002, *Loi relative aux droits du patient*.

⁸³ Defined in EDPB Opinion 3/2019, as processing operations relating to a specific CT, from the ‘starting of the trial to deletion at the end of the archiving period’ (Article 7). Note, that at the same time, consent is not excluded.

⁸⁴ EDPB provides several examples of such power imbalance: “when a participant is not in good health conditions, when participants belong to an economically or socially disadvantaged group or in any situation of institutional or hierarchical dependency.” (EDPB Opinion 3/2019, p. 6); see also a presumably confirmation of this position in the EDPB Guidelines 03/2020, p. 5.

⁸⁵ See Article 58 Clinical Trials Regulation concerning obligations to archive the clinical trial master file for 25 years.

⁸⁶ In particular, Verhenneman argues that informed consent may not be the preferred legal basis when (i) there is lack of freedom (e.g. when signing informed consent for the processing of personal data is a by-product of a service, such as the ability to receive the newest treatment available through the participation in a clinical trial); (ii) there is a lack of information or understanding (e.g. through the use of complicated and very long informed consent documents); (iii) there is lack of specificity (e.g. by considering informed consent as a general waiver to use and secondary use of personal data). See Verhenneman, G., 2020, p. 169, and also p. 110-173.

⁸⁷ See Principle 15(3) of CoE Recommendation CM/Rec(2019)2.

⁸⁸ See e.g., Kamenjasevic, E., ‘*Health data for scientific research under the CoE Recommendation and the GDPR – Part II*’, Blog of KU Leuven’s Centre for IT&IP Law, 2019.

⁸⁹ Ienca, M., et al., 2019. Authors of a stakeholder advisory opinion prepared for an ISC seminar expressed a similar view: ISC Intelligence, ‘The Application of GDPR to Biomedical Research: Stakeholder Advisory Opinion to Assist Regulators, Prepared for the ISC Seminar on Challenges for Health Research Arising from the GDPR’, 19 November 2019, p. 8: “Moreover, the EDPB’s guidance that consent for data processing is not “freely given” in the context of a clinical trial is at odds with standard practice in research ethics, including the Declaration of Helsinki, and the EU’s own Clinical Trials Regulation, both of which typically require obtaining the voluntary consent of research subjects before enrolling them in a clinical trial. The EDPB has never explained why it believes that a research subject’s consent to the processing of personal data in connection with a clinical trial cannot be freely given, whereas consent to participate in the clinical trial itself can be freely given. It is curious for the EDPB to conclude, apparently, that a research subject can consent to receive an investigational medicinal product of unknown safety and efficacy but that another basis for data processing is recommended because of concerns that consent may not be freely given.” ISC is an advisory firm specializing in science, technology and R&D research and policy. They provide intelligence on science and innovation policy and programmes. See more at: <http://iscintelligence.com/aboutisc.php>.

⁹⁰ Van Veen, E., 2018, p. 74 The EDPA provided a similar example in its EDPA Guidelines 03/2020, p. 5, namely a survey which is conducted as part of a non-interventional study on a given population, researching symptoms and the progress of a disease.

⁹¹ See Vanden Heede, E., ‘GDPR Application in Patient Preference Studies’, Master thesis for Intellectual Property and ICT Law under supervision of Prof. Huys, I., p. 23-27. Patient preferences “reflect why patients choose a particular health intervention over other available options. This health treatment can be a drug or a medical device. A preference can be stated for a health intervention as a whole or for the advantages and disadvantages of one intervention. In order to make a choice or state a preference, patients need to weigh up the advantages and disadvantages and compare them to those of other health interventions.”, see Huys, I., ‘Integrating patient preferences in the drug life cycle’, Presentation for the Patient Preferences in Benefit-Risk Assessments during the Drug Life Cycle (PREFER).

⁹² Quinn, P., Quinn, L., ‘Big genetic data and its big data protection challenges’, *Computer Law & Security Review*, Vol. 34, No. 5, 2018, p. 1000-1018 (‘Quinn & Quinn Big Genetic Data 2018’).

⁹³ See e.g. Dove, E., ‘The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era’, *The Journal of Law Medicine and Ethics*, Vol. 46, No. 4, 2018, p. 1013-1030; Verhenneman, G., Claes, K., Derèze, J.J., Herijgers, P., Mathieu, C., Rezda, R., Vanautgarden, M., ‘How GDPR Enhances Transparency and Fosters Pseudonymisation in Academic Medical Research’, *European Journal of Health Law*, Vol. 27(1), Brill and Nijhoff, 2019, p. 40; Quinn, P., ‘The Anonymisation of Research Data — A Pyrric Victory for Privacy that Should Not Be Pushed Too Hard by the EU Data Protection Framework?’, *European Journal of Health Law*, Vol. 24, No. 4, 2017, p. 347-367; van Veen, E., 2018. See also Quinn and Quinn arguing that Consent is not the most reliable option for researchers, especially ones working with Big Data: Quinn, P. & Quinn L., 2018, p. 1013.

⁹⁴ DHallinan, D., ‘Broad consent under the GDPR: an optimistic perspective on a bright future’, *Life Sciences, Society and Policy*, Vol. 16, Springer, 2020, p. 11.

⁹⁵ Interview with Alexandre Entraygues, Head Data Privacy Europe at Novartis, *European Data Protection Law Review*, Vol. 5, No. 5, Lexxion, 2019.

⁹⁶ This is because of 1) the lack of harmonized approach nationally (e.g., if a trial is open in Germany, it would be easier to use consent as a basis everywhere) (see also below), and 2) because they have been using consent for more than 70 years as the standard. On the other hand, and at the same time, it was also shared that there are companies (referred to as “early adopters”), who have started trying to follow the line of the EDPA, but with difficulties. Moreover, in practice, and especially for patients, it is very hard to distinguish between the two types of consent in practice, which leads to a lot of confusion. See the Webinar, Gene, A., Long, W., *Webinar ‘Clinical Trials and GDPR – State of play’*, Drug Information Association (DIA), 10 July 2019. Cole and Towse also argue and assume that pharmaceutical companies would look to their process of obtaining consent as a way to explicitly set out and gain “permission” for all data processing activities. However, they rightfully argue that this may put companies in a more risky position, as achieving the high standards set in the data protection legislation would be difficult in a research context (whether commercial or public), and it implies that no other legitimate basis for using the data is available. See Cole, A. and Towse, A., ‘Legal Barriers to the Better Use of Health Data to Deliver Pharmaceutical Innovation’, *OHE Consulting Report*, 23 (2018), Office of Health Economic, London, 2018, p. 21.

⁹⁷ In particular, the Council of Europe recommendations which were discussed in Section 3.1 of this report, and specifically CoE Recommendation (81)1 on medical databanks, CoE CM/Rec (2019)2 on protection of health-related data, and CoE Recommendation 2016(6) on research on biological materials of human origin.

⁹⁸ In particular, the Council of Europe conventions which were discussed in Section 3.1 of this report, and specifically the CoE Convention 108+.

⁹⁹ Belgium, Bulgaria, Croatia, Cyprus, France, Germany, Greece, Hungary, Italy, Latvia, the Netherlands, Portugal, Romania, Slovakia, Slovenia, and Norway.

¹⁰⁰ Belgium, Bulgaria, Greece, Hungary, Latvia, Portugal, Slovakia, Slovenia, UK, and Norway.

¹⁰¹ For primary genetic testing for scientific purposes (Article 16-10 of the Civil Code and Article 76 *Loi Informatique et Libertés – LIL*, French data protection act). Consent provided in these situations covers the necessary processing of personal health data related to the purpose of the research at the exclusion of processing made mandatory by law such as for obtaining drug marketing authorisation with competent authorities relying on the legal obligation of data controller and/or on the pursuit of a public interest purpose. Article 76 LIL requiring consent prior to genetic examination for research purposes does not apply to researches performed on the basis of already obtained biological samples in the respect of Article L.1131-1-1 PHC.

¹⁰² The Italian data protection act (PDPC) sets two key provisions concerning the legal basis for processing special categories of personal data for scientific research. According to the PDPC, consent as a legal basis for scientific research, is required mainly in two cases: (i) When data concerning health are processed for research purposes in the medical, biomedical and epidemiological field (Article 110 PDPC). In such cases, consent is the legal basis that applies, unless laws or regulations pursuant to Article 9(2)(i) GDPR apply, or when the data processing is carried out within the framework of a national research programme pursuing to Leg. Decr. 502/1990; (ii) When genetic data are processed for research purposes. Section 2(f)(6) PDPC (Safeguards applying to the processing of genetic data, biometric data, and data relating to health) does not require consent as such, i.e. as a default rule for processing genetic data, however the article foresees that the Italian SA may set additional measures, including consent. Following this article, and other relevant rules, the Italian SA, has foreseen additional measures including consent, via decisions and guidelines.

¹⁰³ Section 40(1)(3)c) of the German Medicinal Product Law.

¹⁰⁴ See input for France.

¹⁰⁵ See input for Germany and Italy.

¹⁰⁶ Norms related to the implementation of the rules of good practice in conducting clinical trials performed with drugs for human use, Approved by Decree of the Ministry of Health No. 904/25.07.2006, available at <http://www.scumc.ro/LegisDir/42.%20Ordin%20904%20din%202006.pdf>.

¹⁰⁷ For instance, one stakeholder in clinical research (EORTC) recently stated that their preferred legal basis is Article 6(1)(f) in conjunction with Article 9(2)(j) GDPR. European Organisation for Research and Treatment of Cancer, *EORTC Contribution to the EMA Discussion Paper for Medicines Developers, Data Providers, Research-Performing and Research-Supporting Infrastructures entitled “The General Data Protection Regulation: Secondary Use of Data for Medicines and Public Health Purposes Discussion Paper for Medicines Developers, Data Providers, Research-Performing and Research-Supporting Infrastructures”*, 10 July 2020.

¹⁰⁸ Moreover, the same provides that the legal basis may contain specific provisions related to different elements (lawfulness conditions, types of data to be processed, concerned data subjects, purpose limitation, storage periods). See e.g., Finland, where scientific research is recognised under Article 6(1)(e) GDPR: Section 4, Finnish Data Protection Act, available at: <https://www.finlex.fi/en/laki/kaannokset/2018/en20181050.pdf>.

¹⁰⁹ Kotschy, W., ‘Article 6 Lawfulness of processing’, in Kuner, C., A. Bygrave, L., Docksey, C., (eds.), *The EU General Data Protection Regulation (GDPR). A commentary*, Oxford University Press 2020, p. 335.

¹¹⁰ *Id.*, p. 334.

¹¹¹ Recital 45 GDPR and EDPB Opinion 3/2019, fn. 12, p. 7.

¹¹² *Id.*

¹¹³ Kramer, P., ‘Article 6, Rechtmäßigkeit der Verarbeitung’, in Auernhammer, H., Eßer, M., Kramer, P., von Lewinski, K., (eds.), *Auernhammer DSGVO/BDSG*, 5th ed., Carl Heymanns Verlag, Cologne, 2017, as cited in Kotschy, W., 2020.

¹¹⁴ Kotschy, W., 2020, p. 335.

¹¹⁵ See EORTC Contribution to the EMA Discussion Paper.

¹¹⁶ Article 4(23) GDPR.

¹¹⁷ The same would apply to relying on Article 9(2)(i) GDPR, necessity for reasons of public interest in the area of public health. This exception is a narrow one, and best suited for public health authorities, NGOs, entities working in areas such as disaster relief and humanitarian aid. See also Georgieva, L., and Kuner, C., ‘Article 9 Processing of special categories of personal data’ in Kuner, C., A. Bygrave, L., Docksey C., (eds.), *The EU General Data Protection Regulation (GDPR). A commentary*, Oxford University Press 2020, p. 380.

¹¹⁸ In particular, the Council of Europe recommendations which were discussed in Section 3.1 of this report, and specifically CoE Recommendation (81)1 on medical databanks, CoE CM/Rec (2019)2 on protection of health-related data, and CoE Recommendation 2016(6) on research on biological materials of human origin.

¹¹⁹ In particular, the Council of Europe conventions which were discussed in Section 3.1 of this report, and specifically the CoE Convention 108+.

¹²⁰ It may not be possible to justify it in every Member State, and moreover, as described above, there is still unclarity (at least in the scholarly debate) whether it is possible for commercial entities to rely on it at all.

¹²¹ In support of this conclusion, see the UK Medical Research Council which previously identified this legal basis as the one that UK public bodies (universities, NHS, research councils) are most likely to rely on: see UK Medical Research Council, ‘*Guidance Note 3, General Data Protection Regulation (GDPR): Consent in Research and Confidentiality*’, March 2018, as updated in March 2019.

¹²² See last sentence of Article 6(1) and Recital 47 of the GDPR.

¹²³ Kotschy, W., 2020, p. 337. Hence only a commercial interest would not suffice. Potential sources of legitimate interests are the fundamental rights and freedoms recognized in the Charter of Fundamental Rights of the EU, and examples are also provided in the GDPR recitals.

¹²⁴ Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 844/14/EN, WP 217, 9 April 2014. According to Shabani and Borry, Recitals 47 and 113 provide grounds in support of this understanding, see Shabani, M., Borry, P., ‘Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation’, *European Journal of Human Genetics*, Vol. 26, No. 2, 2018. p. 149-156.

¹²⁵ See Article 29 WP Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, p. 33. These criteria are a) assessing the controller’s legitimate interests, b) impact on the data subjects, c) provisional balance, and d) additional safeguards applied by the controller to prevent any undue impact on the data subjects.

¹²⁶ See Kotschy, W., 2020, p. 344.

¹²⁷ About this recital and the balancing test, see also Ducato, R., ‘Data protection, scientific research, and the role of information’ (CRIDES Working Paper Series no. 1/2020), *Computar Law and Security Review*, 2020.

¹²⁸ In particular, the Council of Europe recommendations which were discussed in Section 3.1 of this report, and specifically CoE Recommendation (81)1 on medical databanks, CoE CM/Rec (2019)2 on protection of health-related data, and CoE Recommendation 2016(6) on research on biological materials of human origin.

¹²⁹ In particular, the Council of Europe conventions which were discussed in Section 3.1 of this report, and specifically the CoE Convention 108+.

¹³⁰ Principle 2(3) of the International Council on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use (ICH) Guideline for Good Clinical Practice E6 (R2), available at: <https://www.ema.europa.eu/en/ich-e6-r2-good-clinical-practice>. See also e.g. Article 3 of the Additional Protocol to the CoE Convention 164 (Oviedo Convention, 1997), concerning Biomedical research.

¹³¹ See European Data Protection Board, Guidelines 3/2019 on processing of personal data through video devices, 10 July 2019, p. 10-11. This intensity can, inter alia, be defined by: the type of information that is gathered (information content), the scope (information density), the number of the data subjects concerned, the situation in question, the actual interests of the group of data subjects, alternative means and the nature and the scope of the data assessment.

¹³² Concerning the compatibility assessment in Article 6(4) GDPR, Recital 50 specifically mentions ‘the reasonable expectations of data subjects based on their relationship with the controller as to their further use’, thus establishing a direct link.

¹³³ EDPB Opinion 3/2019, p. 5. The WP29 also previously clarified that Article 6 and Article 9 should be applied cumulatively, see Article 29 Data Protection Working Party advice on Agreement between National Authorities or National Organisations responsible for National Contact Points for eHealth on the Criteria required for the participation in Cross-Border eHealth Information Services, Brussels, 11th April 2018, p. 2-3.

¹³⁴ Hallinan, D., 2020, p. 23.

¹³⁵ Scholars in Bulgaria and Italy view Article 9 GDPR as the sole legal basis required. See Toshkova-Nikolova, D., Feti, N., *Зашита на личните данни* [Protection of personal data], ИК Труд и Право [Publishing House Trud i Pravo], 2019; see the national input for Italy for this study.

¹³⁶ See the national input for France for this study.

¹³⁷ Netherlands, Ministry of Justice and Security, ‘Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet, Algemene verordening gegevensbescherming’ [Instruction manual General Data Protection Regulation and Implementing Act of the General Data Protection Regulation], 2018.

¹³⁸ Slovakia, Office for Personal Data Protection, Guidelines 2/2018.

¹³⁹ Cyprus, Denmark, Germany, Greece, Latvia, Romania, Portugal, Slovenia, UK, and Norway.

¹⁴⁰ Georgieva, L. and Kuner, C., 2020, p. 380.

¹⁴¹ According to Hallinan, the concept is comparable to ‘important’ public interest for which jurisprudence is available (Hallinan, D., 2020, p. 6, fn. 8). WP29 has previously observed that the latter notion should be given a ‘restrictive interpretation’ and should refer to processing which is necessary and identified as an important public interest by national legislation (Article 29 Data Protection Working Party, Working document on a common interpretation of Article 26(1) of Directive 5/46/EC of 24 October 1995, 2093/05/EN, WP 114, 25 November 2005, p. 14-15). According to the Meszaros & Ho order of the levels of public interest, the ‘substantial’ under 9(2)(g) GDPR is the highest level of public interest referred to under GDPR (Mészáros, J., Ho, C., ‘Big Data and Scientific Research: The Secondary Use of Personal Data under the Research Exemption in the GDPR’, *Hungarian Journal of Legal Studies*, Vol. 59, No. 4, 2018, p. 408). To our knowledge, the provision is implemented in France, see Article 44(6) Loi Informatique et Libertés (LIL) regarding necessary processing performed for public research purposes (as defined under Article L. 112-1 of the Code of Research) and answering to important reasons of public interest on the basis of Art.9(2)(g) GDPR.

¹⁴² The processing must: concern scientific research purposes; be based on and in compliance with Union or Member State law; be proportionate, i.e. the data must be processed only so far as strictly necessary; respect the essence of the right to data protection; provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject. The law does not specify what those safeguards must be. In the lack of specificity, Georgieva and Kuner find that controllers and processors have to design safeguards based on the data protection principles (e.g. proportionality, data minimization). Examples include encryption, minimizing the amount of sensitive data processed, training staff who handle personal data and placing them under a duty of confidentiality. (See Georgieva, L. and Kuner, C., 2020, p. 380).

¹⁴³ Hallinan, D., *Feeding biobanks with genetic data. What role can the general data protection regulation play in the protection of genetic privacy in research biobanking in the EU?*, VUB Doctoral Thesis, Brussels, 2018, p. 323.

¹⁴⁴ Mészáros, J., and Ho, C., 2018, p. 409.

¹⁴⁵ Mészáros, J., and Ho, C., 2018, p. 408.

¹⁴⁶ Article 25(m) of the Personal Data Protection Act (PDPA). The PDPA is available in English at: <https://www.cpdp.bg/en/index.php?p=element&aid=1194>.

¹⁴⁷ Article 10 of Act No. 502 of 23 May 2018 on supplementary provisions to the regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

¹⁴⁸ *Loi Informatique et Libertés (LIL)*, Title II, Chapter I Title II, Chapter III, Section 3 ans *Code de la Santé Publique (PHC)*, Article L. 1121-1 and following ,Article L. 1461-1-V , Article L.1131-1-1, ,Article L. 1461-1 and following.

¹⁴⁹ Article 9(2)(j) GDPR is provided with national legislative support in the new national data protection act implementing the GDPR - BDSG. Conditions legitimating the use of Article 9(2)(j) GDPR are generally outlined in Article 27. Article 27 then points to Article 22(2)(2) which provides a – non-exhaustive – list of safeguards a data controller should implement to protect the rights and freedoms of data subjects. The provisions outlined in Articles 27 and 22, however, are not particularly specific in relation to research or indeed in relation to any types of data processing activity. In this regard, there remain questions as to the degree to which these Articles, alone, fulfil the requirements of Article 9(2)(j) GDPR – in particular as this requires: “Union or Member State law...[to] provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject”.

¹⁵⁰ Law 4624/2019, Article 30: Processing of special categories of personal data is allowed without data subject’s consent when it is necessary for, inter alia, scientific research purposes and the data controller’s interest overrides the data subject’s interest in not having their personal data processed. The article demands that suitable, specific safeguards should be set in place to protect data subjects’ legitimate interests and provides indicative examples.

¹⁵¹ Amendment of the 2011 CXII. Law on the Right to Self-Determination of Information and Freedom of Information was accepted on 16th of July 2018 by the Hungarian Parliament (2011. évi CXII. Törvény az információs önrendelkezési jogról és az információszabadságról), available at: <https://www.parlament.hu/irom41/00623/00623-0008.pdf>. Article 3(7) contains a reference to explicit consent and Article 5 provides a lawful ground for (i) personal data and (ii) sensitive data processing (including) in the context of scientific research.

¹⁵² Article 25 (2) and (3) of the Latvian Data Protection Law (PDPL), available at: <https://likumi.lv/ta/id/300099#p32>. This PDPL provision requires consent for data processing in all cases, also for the purposes of scientific research. Secondary use of data is allowed if there are legal grounds for that as per the GDPR (inter alia, consent), or it must be compatible with the original processing purpose. Article 10(7) on the law of patients data, available at: <https://likumi.lv/ta/en/en/id/203008-law-on-the-rights-of-patients>. The Law on Patients’ Rights allows the secondary use of patient data for research purposes where: (i) the patient cannot be directly or indirectly identified according to the information to be analysed; or (ii) the patient has consented in writing that the information regarding him or her may be used in a specific research, or (iii) permission to process patient

data is granted in a special procedure by a competent authority. It is important to note that although Article 25(2) states that processing of special categories of data is possible if at least one of the grounds referred to in Article 9(2) GDPR exists, including Article 9(2)(j) GDPR, Latvian law does not provide safeguards relating to processing of personal data for scientific purposes as required under Article 89(1) of the GDPR.

¹⁵³ Article 31(4) of Law 58/2019 ensuring execution, in the national legal order, of Regulation (EU) 2016/679.

¹⁵⁴ Article 8, Paragraphs 1, 3 and 4 of the Law No. 190/2018 on implementing measures of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, available at: <https://lege5.ro/Gratuit/gi4dsnjugi2q/legea-nr-190-2018-privind-masuri-de-punere-in-aplicare-a-regulamentului-ue-2016-679-al-parlamentului-european-si-al-consiliului-din-27-aprilie-2016-privind-protectia-persoanelor-fizice-in-ceea-cee-priv>. Article 346, Paragraphs 1 and 4 of the Law No. 95/2006 on health care reform (*Legea nr. 95/2006 privind reforma în domeniul sănătății*), 1 May 2006, available at: <https://lege5.ro/App/Document/g42tmnjsg/legea-nr-95-2006-privind-reforma-in-domeniul-sanatatii?d=22.04.2020&forma=zi>.

¹⁵⁵ Article 16, a and k Data Protection Act, available at: <https://www.zakonypreldi.sk/zz/2018-18>. The article stipules the situation when the prohibition of the processing of special categories of personal data shall not apply if:

(a) the data subject has given explicit consent to the processing of those personal data;

(k) processing is necessary for archiving purposes, for scientific purposes, for historical research purposes or for statistical purposes pursuant to this Act.

¹⁵⁶ Article 110 of the Italian PDPC can be considered an implementation of Article 9(2)(j) GDPR.

¹⁵⁷ Article 9(2)(j) GDPR has been implemented via the UK Data Protection Act 2018. Paragraph 4 of Schedule 1 clarifies that the general prohibition on the use of sensitive data is lifted for the processing of sensitive data for scientific research purposes provided the conditions in Schedule 4, Part 1(4) of the Act are fulfilled. The conditions laid out in this Part, however are limited and, for the most part, simply mirror those in Article 89(1) GDPR. The Part does however, specifically require that research be: ‘in the public interest’. Part 2, Chapter 2, Section 19 also includes clarifications of circumstances which will not fulfil the requirements of Article 89(1) – including if processing “*is likely to cause substantial damage or substantial distress to a data subject*” or if it “*is carried out for the purposes of measures or decisions with respect to a particular data subject*”. The Act raises the same issues as (Germany) BDSG(neu). It is far from clear that the Act alone constitutes a law, according to Article 9(2)(j) GDPR, which provides “*suitable and specific measures to safeguard the fundamental rights and the interests of the data subject*”.

¹⁵⁸ Article 10 of Act No. 502 of 23 May 2018 on supplementary provisions to the regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

¹⁵⁹ Section 6(3)-(6), Estonian Personal Data Protection Act Implementation Act, available at: <https://www.riigiteataja.ee/en/eli/523012019001/consolidate>.

¹⁶⁰ Health Research Act (Lov om medisinsk og helsefaglig forskning), available at: <https://lovdata.no/dokument/NL/lov/2008-06-20-44>. Chapter 7, Sections 32 and 33: prior approval from the ethics committee is deemed to be a necessary and adequate legal basis to process personal health data in medical and health research.

¹⁶¹ Autoriteit Persoonsgegevens, *Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming*, 2018, 43, available at: <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/handleidingalgemeneverordeninggegevensbescherming.pdf>

f. “*Bijzondere categorieën van persoonsgegevens mogen worden verwerkt als dit noodzakelijk is voor wetenschappelijk of historisch onderzoek of statistische doeleinden. Dit mag echter alleen als het onderzoek een algemeen belang dient, het vragen van uitdrukkelijke toestemming onmogelijk blijkt en voldoende waarborgen zijn getroffen om zo min mogelijk risico's voor de persoonlijke levenssfeer van de betrokkenen te creëren*”.

¹⁶² See e.g. ISC Intelligence in Science Input Paper.

¹⁶³ See e.g. an overview prepared by the UK Information Commissioner’s Office, available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/>.

¹⁶⁴ See EORTC Contribution to the EMA Discussion Paper.

¹⁶⁵ ISC Intelligence in Science Input Paper.

¹⁶⁶ Ienca, M., et al., 2019, p.33.

¹⁶⁷ Negrouk, A., Lacombe, D., 2018, p. 1278.

¹⁶⁸ See EORTC Contribution to the EMA Discussion Paper.

¹⁶⁹ Cole, A., Towse, A., 2018.

¹⁷⁰ For instance, the authors of a report prepared for the European Parliament’s STOA panel strongly recommended that ethics committees should help guiding the development of organizational strategies for when to rely on different grounds of lawful processing (see Ienca, M., et al., 2019, p. 33). Verhenneman et al. also stressed the importance of ethics committee reviews as a good organizational measure to protect data subjects in research. The UZ Leuven GDPR compliance policy implemented independent ethics review as a general measure applicable to all research projects (see Verhenneman et al., 2019). Moreover, Verhenneman et al. opine that an ethics review can assess claims about the use of anonymization techniques. This stance comes at odds with the opinions of other researchers.

¹⁷¹ The only reference to ethical standard is found in Recital 33 GDPR, but the recital does not elaborate on ethics committees per se.

¹⁷² Chapter 2, Paragraph 6(2) of the Personal Data Protection Act, available in English at: <https://www.riigiteataja.ee/en/eli/523012019001/consolidate>.

¹⁷³ Section 110 of the Italian Personal Data Protection Code.

¹⁷⁴ Principle 5 of the International Council on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use (ICH) Guideline for Good Clinical Practice E6 (R2), available at: <https://www.ema.europa.eu/en/ich-e6-r2-good-clinical-practice..>

¹⁷⁵ Article 24 GDPR.

¹⁷⁶ Principle 2.3 of the International Council on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use (ICH) Guideline for Good Clinical Practice E6 (R2), available at: <https://www.ema.europa.eu/en/ich-e6-r2-good-clinical-practice>, also e.g. Article 3 of the Additional Protocol to the Convention on Human Rights and Biomedicine (Oviedo Convention), concerning Biomedical research.

¹⁷⁷ World Health Organisation, Operational guidelines for Ethics Committees that review biomedical research, Geneva, 2000.

¹⁷⁸ Hijmans, H., Raab, C.D, ‘Ethical Dimensions of the GDPR’, in Cole, M., Boehm, F., (eds.), *Commentary on the General Data Protection Regulation*, Edward Elgar, Cheltenham, 2018 (forthcoming).

¹⁷⁹ Recital 18 Clinical Trials Regulation: “(...) When determining the appropriate body or bodies, Member States should ensure the involvement of laypersons, in particular patients or patients’ organisations.”.

¹⁸⁰ See <http://www.eurecnet.org/index.html>.

¹⁸¹ The initiative is part of the three-year priority project Nordic Council, ‘*Nordic research collaboration for better health*’.

¹⁸² See Verhennenman, G., 2020, p. 203.

¹⁸³ Similar criticism has been voiced by other scholars, e.g. Hert, P., Papakonstantinou, V., ‘The new general data protection regulation: Still a sound system for the protection of individuals’, *Computer Law and Security Review*, Vol. 32, No. 2, 2016, p. 186; Kuner, C., Svantesson, D.J., Cate, F.H., Lynskey, O., Millard, C., ‘The language of data privacy law (and how it differs from reality)’, *International Data Privacy Law*, Vol. 6, No. 4, 2016, p. 259.

¹⁸⁴ Crucial exception in the view of Borgesius and Hallinan is the case *Österreichischer Rundfunk*, in which the court found that national law derogating from the purpose limitation principle is permissible only if the derogation and the secondary processing are proportionate to the aims it intends to achieve. See C-465/00, C-138/01 and C-139/01 *Rechnungshof* (C-465/00) and *Österreichischer Rundfunk, Wirtschaftskammer Steiermark, Marktgemeinde Kaltenleutgeben, L und Niederösterreich, Österreichische Nationalbank, Stadt Wiener Neustadt, Austrian Airlines, Österreichische Luftverkehrs-AG*, and between *Christa Neukomm* (C-138/01), *Joseph Lauermann* (C-139/01) and *Österreichischer Rundfunk*, [2003], para. 59. See also Kostadinova, Z., ‘Purpose limitation under the GDPR: can Article 6(4) be automated?’, Tilburg University Master Thesis, p. 51-59. The author concluded that the CJEU has not assessed (so far) further processing directly, but it has acknowledged that processing of personal data has to comply with the purpose limitation principle. Furthermore, the CJEU has not yet provided additional knowledge on how to interpret Article 6(4) GDPR. See also Kostadinova, p. 60 for a summary of knowledge obtained from case law on processing of personal data.

¹⁸⁵ Recital 33 has several areas of uncertainty, as outlined by Hallinan. First, the concept ‘certain areas of research’ could be interpreted both narrowly (e.g. only specific types of genomic research, cancer research etc), or broadly (e.g. all types of biological research). Second, it is unclear to which ‘ethical standards’ the recital refers: national instruments governing research, international standards, or standards imposed by ethics committees. Finally, ‘to the extent allowed by the intended purposes’ may be interpreted narrowly (consent can be given only to the narrowest possible use of data), or broadly (data subjects may be given a range of choices of consent options: from narrowest possible use to broader formulations). Hallinan, D., 2018, p. 387-388.

¹⁸⁶ Verhennenman, 2020, p. 211.

¹⁸⁷ Verhennenman, 2020.

¹⁸⁸ Article 29 Working Party, Guidelines on consent under Regulation 2016/679, 2017, p. 28.

¹⁸⁹ Hallinan, D., 2020, p. 28.

¹⁹⁰ European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, 4 May 2020, p. 30-31.

¹⁹¹ Hallinan, D., 2020, p. 13.

¹⁹² Belgium, Germany, Greece, Norway, Italy, Portugal, and UK.

¹⁹³ In the explanatory memorandum to the Belgian Law on the processing of personal data of 30 July 2018 (“*Wet betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens*”) it is noted that data controllers may use Recital 33 in the context of scientific research to for example request consent for “cancer research”, but not “research” or “medical research” (cf. input from Verhennenman, G.).

¹⁹⁴ Department Guidelines on medical and health research (*Veileder til lov 20. juni 2008 nr. 44 om medisinsk og helsefaglig forskning*) clarify that broad consent cannot be given to “all medical research” or to “genetic research”. Rather, it should be possible to give a broad consent to, for example, cancer research or diabetes research, without the individual details required.

¹⁹⁵ The *Datenschutzkonferenz*, in line with the Article 29 Working Party’s clarification on Recital 33, clarify that broad consent is only possible under certain conditions: (i) when the purpose of research really cannot be defined in advance; (ii) when specific measures to mitigate the lack of transparency which comes with broad consent are put in place; (iii) when measures to increase trust – such as ethics committee approval are in place and a consideration of whether granular consent approaches, such as dynamic consent, has been undertaken; and (iv) increased data security measures have been enacted. How far this recommendation will influence practice remains to be seen. Germany, Conference on Data Protection (Datenschutzkonferenz), ‘Beschluss der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung“ im Erwägungsgrund 33 der DS-GVO’, 2019.

¹⁹⁶ Health Research Act (*Lov om medisinsk og helsefaglig forskning*), Chapter 4, Section 14: “*Research participants may consent to the use of their human biological material and health information for specific, broadly defined research purposes. The regional committee for medical and health research ethics may set conditions for the use of broad consent and may require the project manager to obtain new consent if the committee deems it necessary. Participants who have given broad consent are entitled to regular information about the project*”.

¹⁹⁷ Last Bill of bioethics law, projet de loi n°2658.

¹⁹⁸ Article 31(4) of Law No. 58/2019 ensures execution, in the national legal order, of Regulation (EU) 2016/679.

¹⁹⁹ Frunză, A., Sandu, A., ‘Ethical Acceptability of Using Generic Consent for Secondary Use of Data and Biological Samples in Medical Research’, *Acta Bioethica*, Vol. 23, No. 2, 2017, p. 289-299.

²⁰⁰ See the national input for France for this study.

²⁰¹ 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. 31-50).

²⁰² Albeit with more precision by now referring to ‘archiving purposes in the public interest, scientific or historical research purposes or statistical purposes’: Art. 5(1)(b) GDPR. About the purpose limitation principle, see also: Zuiderveen Borgesius, F., Hallinan, D., ‘Article 5’, in Boehm, F., Cole, M., (eds), GDPR Commentary, Elgar, 2021 (forthcoming), (‘Zuiderveen and Hallinan, Article 5 (2021)’).

²⁰³ See also Recital 50 GDPR: “[...] In any case, the application of the principles set out in this Regulation [...] should be ensured [...]”. As to the information obligation, this is confirmed for ‘further processing’ in Article 13(3) GDPR.

²⁰⁴ Article 29 Data Protection, Working Party, Opinion 03/2013 on purpose limitation, 00569/13/EN, WP 203, 2 April 2013, (‘Article 29 WP, WP203’).

²⁰⁵ In this sense, ‘further processing’ shall always be for further, compatible processing and further processing should hence be understood as processing for compatible purposes.

²⁰⁶ Article 29 WP, WP203, p. 21 and p. 28.

²⁰⁷ EDPB Guidelines 03/2020, p. 6.

²⁰⁸ See the original formulation in the Directive 95/46/EC, Article 6(1)(b).

²⁰⁹ See also Recital 50. See also Article 6(4) GDPR, referring to Article 23(1) GDPR, but also allowing, however, national or Union law’s exceptions to the rights of data subjects, including in case of data breach, and Article 5 GDPR (including the purpose limitation principle).

²¹⁰ Hence, the need for safeguards to be determined by national law, including e.g. anonymisation and pseudonymisation. See also Article 29 WP, WP203, p. 28 *et seq.*.

²¹¹ Expectations of the data subjects remain crucial. See also Recital 47: “*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.*” Note that both consent and Union or Member State law are exceptions to the requirement for compatibility: Recital 50, second paragraph and Article 6(4) GDPR. Interestingly, the original Commission Proposal for the GDPR opened up the possibility for further processing for incompatible purposes much more widely, by proposing that further processing should be allowed if done by the same controller and provided that the controller’s or a third party’s legitimate interests prevailed over the data subject’s interests. This idea was heavily criticized (see and as discussed in de Terwagne, C., ‘Article 5 Principle relating to processing of personal data’, in Kuner, C., A. Bygrave, L., Docksey, C., (eds.), The EU General Data Protection Regulation (GDPR). A commentary, Oxford University Press 2020, p. 316). Recital 47 (see also below) could be a remnant.

²¹² See also Recital 50 GDPR: “[...] Union or State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful”.

²¹³ See EDPB, *Guidelines 4/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*, 21.4.2020, European Data Protection Board, Guidelines 4/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, 21 April 2020, Article 21.

²¹⁴ See also Recital 34 GDPR in this regard. In the case *ECtHR, S. and Marper v. U.K. [GC], Applications No. 30562/04 and 30566/04, 4 December 2008*, the court clearly stated that ‘all three categories of the personal information retained by the authorities (...) and cellular samples, constitute personal data within the meaning of the Data Protection Convention as they relate to identified or identifiable individuals.’ (emphasis added). The opponent, the U.K. government also clearly accepted that all three categories are ‘personal data’ within the meaning of the UK Data Protection Act in the hands of those who are able to identify the individual (§ 68). On this subject, see also Bygrave, L.A., ‘The Body as Data? Biobank Regulation via the ‘Back Foot’ of Data Protection Law’, *Law, Innovation and Technology*, Vol. 2, No. 1, 2010, p. 1-25, p. 3. The author states that it is not impossible to apply data protection legislation to biological material. He mentions the New South Wales Privacy and Personal Information Protection Act 1998, which defines ‘personal information’ as encompassing, *inter alia*, ‘body samples’ (section 4). He also refers to the discussion in Norway and to the report ALRC, *Essentially Yours*, 2003; see Bygrave, L.A., 2010, p. 1-25 and Kindt, E., *Privacy and Data Protection Issues of Biometric Applications*, Springer, 2013, pp. 179-189.

²¹⁵ Recital 34 GDPR defines genetic data 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*”.

²¹⁶ In Germany: See, for example: Herbst, T., ‘Art. 5 Grundsätze für die Verarbeitung personenbezogener Daten’, in Kühling, J., Buchner B. (eds.), *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG*, 228, Beck, 2018: a new legal basis is necessary; Reimer, P., ‘Artikel 5: Grundsätze für die Verarbeitung personenbezogener Daten’ in Sydow, G., (ed.), *Europäische Datenschutzgrundverordnung: Handkommentar*, Nomos, 2018, 326: no new legal basis is necessary; Germany, Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, *Public Consultation on the theme: Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche*, 2020, p. 6-7: the original legal basis could serve as the basis for the secondary processing.

²¹⁷ EDPS, A Preliminary Opinion on data protection and scientific research, p. 22-23.

²¹⁸ European Commission, Question and Answers on the interplay between the Clinical Trials Regulation and the General Data Protection Regulation, p. 8.

²¹⁹ EDPB Opinion 3/2019, p. 8. Until mid-2020, no substantive discussion on the presumption of compatibility was further noted. For example, in the report prepared for the STOA panel of the European Parliament, the need of a new legal basis for secondary use was not discussed. Among the conclusions was that both EDPB and national regulatory bodies should establish how data might be reused for secondary scientific reasons pursuant to Articles 6 and 9: Ienca, M., et al., 2019, p. 38.

²²⁰ European Medicines Agency (EMA), *The General Data Protection Regulation: Secondary Use of Data for Medicines and Public Health Responses. Discussion Paper for Medicines Developers, Data Providers, Research-Performing and Research-Supporting Infrastructures*, 2020, p. 9. The paper is part of a project conducted by EMA in collaboration with the European Milieu Consulting SPR

Study on the secondary use of personal data in the context of scientific research Brussels

Commission. The project aims to develop “Questions and Answers (Q&As) on the GDPR and the Secondary Use of Data for Medicines and Public Health Purposes.” The discussion paper was sent to interested stakeholders who were invited to share their experience and questions on 9 key topic areas, namely secondary use of health data, legal basis, presumption of compatibility, pseudonymisation, data retention, transparency, data subjects' rights, registries, and international transfers.

²²¹ EORTC Contribution to the EMA Discussion Paper.

²²² Kotschy, W., 2020, p. 341.

²²³ Zuiderveen Borgesius, F., Hallinan, D., 2021. See further also Verhenneman, who stated that the “*GDPR creates a favorable position for scientific research, not by excluding the requirement for a compatibility test, but by limiting the compatibility assessment to an assessment of the appropriate safeguards*”: Verhenneman, G., et al., 2019, p. 40

²²⁴ Moreover, the lack of need of a separate legal ground is only partial correct and only in some situations, in that it is possible that ‘further processing’ would not need a new legal ground, but it may well be that a new ground is needed in other situations.

²²⁵ See also Zuiderveen Borgesius, F., Hallinan, D., 2021.

²²⁶ Charter of Fundamental Rights of the European Union (OJ C 326, 26.10.2012), p. 391–407.

²²⁷ See also, in the same sense, in particular for ‘medical research’, EDPB Guidelines 03/2020, p. 5.

²²⁸ E.g., in Finland (see also below). In Finland, for example, secondary purpose is therein defined as ‘the processing of personal data for a purpose other than the primary purpose’. Primary purpose is defined as referring to ‘the purpose for which the personal data was originally saved’: Sec.3(2) and (3) Finnish Act on Secondary Use of Health and Social Data (non-official English translation).

²²⁹ In which case it could be possible to process on the same legal ground, while at the same time a new legal ground may also be required (see above).

²³⁰ In which case always a (new) legal ground shall be ascertained.

²³¹ Bulgaria, Croatia, Cyprus, Denmark, France, Germany, Latvia, Romania, Slovakia, Slovenia, Norway, Portugal.

²³² Germany, Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Public Consultation on the theme: Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, 2020, p. 6-7.

²³³ Belgium, Hungary, Greece, Italy.

²³⁴ Law 4624/2019, Official Government Gazette A’ 137/29.08.2019, <http://www.et.gr/idocs-nph/search/pdfViewerForm.html?args=5C7QrtC22wFqnM3eAbJzrXdtvSoClrL8WkQtR1OJjDd5MXD0LzQTLWPU9yLzB8V68knBzLCmTXKaO6fpVZ6Lx9hLsIJUqeIQFO1o1b-ZCxkj8oDGZfpPVRON0QvoraqawUQAqlqKetE>. See also EXPLANATORY MEMORANDUM to the Draft Law “Hellenic Data Protection Authority, Implementation Measures of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and Transposition into National Legislation of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016”. Note that the relevant provisions have been criticised by the Greek SA. Hellenic Data Protection Authority, ‘Opinion No. 1/2020.’

²³⁵ Verhenneman, G., et al., 2019, p. 40.

²³⁶ P Aurucci, P., ‘Legal issues in regulating observational studies: The impact of the GDPR on Italian biomedical research’, *European Data Protection Law Review*, Vol. 5, No 2, Lexxion, 2019, p. 206.

²³⁷ Section 110-a of the new Italian Data Protection Act (PDPC), available in English at: <https://www.garanteprivacy.it/documents/10160/0/Data+Protection+Code.pdf/7f4dc718-98e4-1af5-fb44-16a313f4e70f?version=1.3>.

²³⁸ According to Article 22(4) of Legislative decree no 101 of 10 August 2018, the general authorisations referred to in Article 40 of the old PDPC are to be maintained for a transitional period.

²³⁹ Section 100 PDPC.

²⁴⁰ UK Information Commissioner’s Office, Overview ‘*Lawful Basis for Processing*’.

²⁴¹ UK Medical Research Council, ‘GDPR: Answers to some frequently asked questions (FAQs) - Can I share data with colleagues now that GDPR is in force?’.

²⁴² Belgium, Bulgaria, Croatia, France, Hungary, Romania, Germany, Slovenia, Norway, Portugal.

²⁴³ 2019 CXXIII. Act amending the LXXVI of 2014 Act and certain related legal provisions on Scientific Research, Development and Innovation – 2019, évi CXXIII. törvény a tudományos kutatásról, fejlesztésről és innovációról szóló 2014. évi LXXVI. törvény és egyes kapcsolódó törvényi rendelkezések módosításáról, available at: <https://mkogy.jogtar.hu/jogsabaly?docid=A1900123.TV>.

²⁴⁴ See the national input for France for this study.

²⁴⁵ Romanian Law on health care reform.

²⁴⁶ Verhenneman, G., et al., 2019, p. 40.

²⁴⁷ Toshkova-Nikolova, D., Feti, N., 2019, p. 94.

²⁴⁸ Greece, Slovakia, UK, Italy, Portugal.

²⁴⁹ See Comande, G., ‘Ricerca in Sanità e Data Protection un Puzzle...Risolabile’, *Rivista italiana di medicina legale e del diritto in campo sanitario*, Vol. 1., 2019, p. 187-207.

²⁵⁰ Under the supervision of the Ministry of Social Affairs and Health.

²⁵¹ See Act on the Secondary Use of Health and Social Data (552/2019), which entered into force on May 1, 2019, available at the Finnish Ministry of Social Affairs and Health, Secondary use of health and social data, <https://stm.fi/en/secondary-use-of-health-and-social-data> with short summary and link to the Act. The main objectives of the Act include the easier, secure and more efficient access and use of health and social care data for various secondary use purposes in the field of scientific research and statistics, besides other purposes such as ‘development and innovation activities’ and supervision and reporting, while guaranteeing the data subject’s legitimate expectations and rights and freedoms (Section1).

²⁵² See <https://www.findata.fi/en/>.

²⁵³ The data will only be provided via a secure information processing environment approved or provided by FinData (see Section 20 *et seq.*), enabling remote access to the raw data, without downloading or export possibilities. Outside this *Milieu Consulting SPR Study on the secondary use of personal data in the context of scientific research Brussels*

environment, only irreversibly aggregated data (done by FinData) may be processed. This approach has been criticized as possibly impeding (international) research initiatives: see Southerington, T., ‘GA4GH GDPR Brief: The Finnish Secondary Use Act 2019 (May 2020 Bonus Brief)’ [blog post], 21 May 2020.

²⁵⁴ “Knowledge management refers to the processing of data carried out by a service provider in their customer, service and production processes for the purpose of supporting operations, production, financial control, management and decision-making” (Section 3(5)). See also Section 41.

²⁵⁵ In particular for promotion of public health or social security, to develop social and health care services or protect the health or wellbeing of individuals.

²⁵⁶ Belgium, Bulgaria, Croatia, Cyprus, France, Germany, Greece, Hungary, Italy, Latvia, Netherlands, Portugal, Romania, Slovakia, Slovenia, and Norway.

²⁵⁷ World Medical Association, *International Code of Medical Ethics*, 1949, last amended in 2006: The Internaitonal Code of Medical Ethids of the World Medical Association was adopted by the 3d WMA General Assembly in October 1949, and last amended by the 57th WMA General Assembly in October 2006.

²⁵⁸ CoE Recommendation (81) 1, Article 5(4): “Without the data subject's express and informed consent, the existence and content of his medical record may not be communicated to persons or bodies outside the fields of medical care, public health or medical research, unless such a communication is permitted by the rules on medical professional secrecy”.

²⁵⁹ UK Secretary of State for Health and Social Care, Decision ‘Coronavirus (COVID-19): notice under regulation 3(4) of the Health Service (Control of Patient Information) Regulations 2002 – general’, 29 July 2020. It may be extended by further notice.

²⁶⁰ It has also no equivalent in other key pieces of EU legislation (Electronic Privacy Directive 2002/58/EC, Law Enforcement Directive (EU) 2016/60). It has an equivalent only in the Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the EU institutions, bodies, offices and agencies (Article 12) and the two provisions should be interpreted homogeneously, pursuant to its Recital 5.

²⁶¹ Note that there was also no mention of it in the report prepared for the STOA panel of the European Parliament in 2019: Ienca, M., et al., 2019.

²⁶² See also Recital 64 GDPR: “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”.

²⁶³ This is a conclusion reached by a joint reading of the text of Articles 4, 5 and 11 GDPR, Recital 26 GDPR (concerning personal data) and Article 29 Data Protection Working Party, Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Systems (C-ITS), 17/EN, WP 252, 4 October 2017.

²⁶⁴ See e.g. Georgieva, L., Kuner, C., 2020, p. 394-396. She states *inter alia*: “Article 11 applies when the controller holds personal data but some informational elements are missing and the controller cannot (any longer) identify the data subject.” (p. 396). See also Toshkova-Nikolova, D., Feti, N., 2019, p. 144 et seq. See also Hintze, M., ‘Viewing the GDPR through a De-Identification Lens: A Tool for Compliance, Clarification, and Consistency’, *International Data Protection Law*, Vol. 8, No. 1, Oxford University Press, 2018, p. 86-101. There are, however, other views (see also national input, especially for France and Belgium).

²⁶⁵ According to Georgieva, Article 11 GDPR could be seen as concerning a principle, because it is in the same chapter as Articles 4-6. If this is accepted, it would mean that the article has *de jure* potential impact on each GDPR provision which requires identification, but *de facto* it impacts only on Articles 15-20, pursuant to its Paragraph 2. See: Georgieva, L., 2020, p. 394. There are other opinions, however. For instance, that Article 11(1) GDPR applies to the obligations pursuant to Articles 13 and 14, stating that these obligations do not have to be fulfilled when Article 11 applies. See: Gola, P., ‘Article 11’, *Datenschutz-Grundverordnung: DS-GVO, VO (EU) 2016/679*, 2nd Edition, C.H. BECK, 2017, para 8 as cited in Georgieva, L., and Kuner, C., ‘Article 11 Processing which does not require identification’, in Kuner, C., A. Bygrave, L., Docksey C., (eds.), *The EU General Data Protection Regulation (GDPR). A commentary*, Oxford University Press 2020, p. 395.

²⁶⁶ However, WP29 rejected any interpretation aimed at reducing the responsibility of controllers for compliance with data protection obligations. It advised that Article 11 GDPR should be interpreted as ‘a way to enforce “genuine” data minimisation, without... hindering the exercise of data subjects' rights’. See: Article 29 WP Opinion 03/2017, p. 6. This, however, has raised concerns about the risks of re-identification, especially when processing health data. See: Goergieva, L., Kuner, C., 2020, p. 39.

²⁶⁷ Georgieva, L., Kuner, C., 2020.

²⁶⁸ Georgieva, L., 2020, p. 396.

²⁶⁹ Article 8(2) Charter of Fundamental Rights states that ‘data must be processed fairly’ and that everyone ‘has the right of access to data’ and ‘the right to have it rectified’.

²⁷⁰ Here, the Belgian Data protection law is a very relevant example. See 30 Juillet 2018 *Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*, Article 194 which stipulates that where ‘the personal data have not been collected from the data subject, the data controller (Controller 2) concludes an agreement with the initial controller (Controller 1). In case the data are publicly available or there is no other legal requirement to conclude such an agreement, Controller 2 has a duty to notify Controller 1. In any case, Controller 2 is obliged to inform the initial Controller 1 about eventual restrictions on data subjects' rights’. According to Ducato, the underlying assumption of the law is that the initial controller acts as a “contact point” for the data subjects and will fulfil their requests if they want to exercise their rights. See: Ducato, R., 2020. For a similar reading, see also EORTC Contribution to the EMA Discussion Paper: “when (...) receiving controller can easily justify that conditions of Articles 11(1) and 14(5)(b) are met, which releases them from many GDPR obligations, EORTC puts in place additional clauses aiming to further protect data subject rights. Namely, through this agreement, EORTC requires assistance from the recipient controller in case of relevant data subject requests and prompt feedback in case of any high-risk data breach or in case of incidental findings”.

²⁷¹ Possible definition of ‘retrospective research’: “*In a retrospective study, in contrast to a prospective study, the outcome of interest has already occurred at the time the study is initiated.*” See Encyclopedia of Research Design, Neil J. Salkind, N.J. (ed.), SAGE Publications, Inc., 2010.

²⁷² ‘Lost to follow-up’ means a person who has not returned for continued care or evaluation (e.g. because of death, disability, relocation, or drop-out). See: Medical Dictionary, Definition of “Lost to follow-up”, Medical Dictionary, Farlex and Partners, 2009.

²⁷³ Croatia, Cyprus, Germany, Greece, Hungary, Italy, Latvia, Romania, Slovakia, and Norway. Note that Slovenia has not yet adopted a new data protection act pursuant to the GDPR due to its political situation.

²⁷⁴ See contribution for Germany.

²⁷⁵ Section 5.5 “Communication and diffusion” of Garante decision of 5 June 2019. See also contribution for the study for Italy.

²⁷⁶ UK Research Authority, ‘Transparency’ [webpage], last updated in 2018. See also contribution for this study by Dara Hallinan.

²⁷⁷ Toshkova-Nikolova, D., Feti, N., 2019, p. 144. See also contribution for this study by Teodora Lalova.

²⁷⁸ See contribution for this study for France.

²⁷⁹ See contribution for this study for Belgium.

²⁸⁰ In the illustrative case of *Bărbulescu v. Romania*, the European Court of Human Rights (ECtHR) concluded that transparency on the purpose and extent of the processing is a prerequisite for any lawful limitation to the right to privacy. See: ECtHR, *Bărbulescu v. Romania* [GC], Application No. 61496/08, 5 September 2017, CE:ECHR:2017:0905JUD006149608.

²⁸¹ In the case of *I. v. Finland*, the European Court of Human Rights explained that data subjects may not be deprived from their ability to enforce their right to privacy, by not providing transparent information on the processing of their data. The court considered that a lack of transparency with regard to the extent of the data processing deprives individuals from their ability to even prove that their right to privacy was infringed on. The Court found that transparent control mechanisms, such as a log, which would have allowed to perform a retrospective check compliance with Article 8 European Convention on Human Rights (ECHR), should have been available. See ECtHR, *I. v. Finland*, Application No. 20511/03, 17 July 2008, CE:ECHR:2008:0717JUD002051103.

²⁸² European Data Protection Supervisor, Opinion 7/2015, ‘Meeting the challenges of big data, A call for transparency, user control, data protection by design and accountability’, 19 November 2015, p. 8; Gellman, R., ‘Privacy: Finding a Balanced Approach to Consumer Options’, *Robert Gellman webpage*, 2002.

²⁸³ Article 14(5)(b) GDPR.

²⁸⁴ Generally, these platforms are extremely safe and are using advanced access rights management policies which ensure a low risk for information ending up with the wrong data subject – something which is an actual risk when sending information notices through mail or e-mail, especially in research populations with a high mortality rate. Enhancing transparency through patient portals can end discussions on (i) whether or not providing transparency involves a disproportionate effort; and (ii) the non-sense of replacing the right to information of the data subject with publishing general information on a publicly available website.

²⁸⁵ This is proposed by EORTC: “*Instead of having one portal for searching clinical trials and another for device or IVD related studies, EU shall have one single repository where all research, prospective, retrospective, interventional or not, involving humans will be referred to with links between projects if data are re-used. This will not cover all uses of data, as some uses, as mentioned before are not research projects. However, such repository would be beneficial to both data subjects and researchers and will help compliance with many legislations and recommendations*”. See EORTC Contribution to the EMA Discussion Paper.

²⁸⁶ See the national input for UK in this study.

²⁸⁷ See the national input for Belgium in this study.

²⁸⁸ German Association for Medical Informatics, Biometry and Epidemiology (GMDS) and German Association for Data Protection and Data Security (GDD), ‘Datenschutzrechtliche Anforderungen an die medizinische Forschung unter Berücksichtigung der EU Datenschutz-Grundverordnung (DS-GVO)’, 30, 2018.

²⁸⁹ Contribution for France.

²⁹⁰ See also the contributions for Italy for this study. The authors provide other indirect relevant references.

²⁹¹ In this sense, see De Terwagne C., Degraeve É., Delforge A., & Gerard L., *La protection des données à caractère personnel en Belgique: manuel de base*, Politeia, Brussels, 2019, p. 124-130.

²⁹² The cascade is based on measures found in the strategy for GDPR compliance developed by the University Hospitals Leuven and in the old Belgian data protection framework. See Verhenneman, G., et al., 2019. Old Belgian Royal Decree of 13 February 2001, “Koninklijk besluit ter uitvoering van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, BS 13 Maart 2001. See also the elaboration on the cascade by Verhenneman, G., 2020, p. 258.

²⁹³ A relevant question remains when one can speak of ‘anonymised medical data’. Currently (with the Breyer case) the CJEU has adopted a “relative” approach towards anonymization, i.e. considers the necessary effort that would be required by the data controller to identify the data subject and only realistic chances of combining data to identify an individual would be taken into account. Similar view could be found in the old Article 29 Data Protection Working Party, Opinion 04/2007 on the concept of personal data, 01248/07/EN, WP 136, 20 June 2007, (under DPD), where the WP29 used a clinical trials example and it seemed that key-coded data is anonymous in the hands of a third party that does not have access to the key: “*The identification of patients is thus embedded in the purposes and the means of the processing. In this case, one can conclude that such key-coded data constitutes information relating to identifiable natural persons for all parties that might be involved in the possible identification and should be subject to the rules of data protection legislation. This does not mean, though, that any other data controller processing the same set of coded data would be processing personal data, if within the specific scheme in which those other controllers are operating re-identification is explicitly excluded and appropriate technical measures have been taken in this respect.*” Note that the *Privacy Shield* (now invalidated, *CJEU, Judgement of 16 July 2020, Facebook Ireland Milieu Consulting SPR*) Study on the secondary use of personal data in the context of scientific research Brussels

and Schrems, C-311/18, EU:C:2020:559) treated key-coded data as anonymised if the recipient does not possess the key to re-identify the data (Annex II, Article 2(14)(g)). However, Recital 26 GDPR veers towards **an absolute approach**. See also Zuiderveen Borgesius, F., ‘Singling Out People without Knowing Their Names - Behavioural targeting, pseudonymous data, and the new Data Protection Regulation’, *Computer Law & Security Review*, Vol. 32, No. 2, 2016, p. 267.

²⁹⁴ An example thereof is a longitudinal research. Because at regular intervals data need to be collected from the same individuals, it is required to re-establish the link between the individual and the corresponding pseudonym.

²⁹⁵ The use of identifiers is for example required in a cohort study, which is a type of medical research used to investigate the causes of disease and to establish links between risk factors and health outcomes.

²⁹⁶ If that is the case, the transparency obligations should be with the party who anonymises the information. In practice, data subjects will be informed of the further use of their data only when the data are anonymised during the research project. E.g. they are first collected with identifiers, but before the data are analysed, they are anonymised.

²⁹⁷ It rarely happens that this first controller will inform data subjects on the fact that it anonymised the data before transferring them to another controller. While it would be useful for data controllers to keep track of transfers of anonymised data in a register, informing the data subjects individually and for each new purpose on the mere fact of the anonymisation, may not be necessary.

²⁹⁸ See also European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 2 September 2020, p. 20.

²⁹⁹ See European Medicines Agency, Guideline for good clinical practice E6(R2), 1 December 2016.

³⁰⁰ Bulgaria, Croatia, Cyprus, France, Greece, Hungary, Latvia, Romania, and Norway.

³⁰¹ Germany, Slovakia, Slovenia, and the UK.

³⁰² Article 27(3) BDSG(neu). The Article requires controllers to: (i) anonymise data, as soon as this is possible according to the research purposes – unless research subject interests stand in the way; (ii) until anonymisation, data should be pseudonymised, and only processed in unpseudonymised form when this is required by the purposes of research.

³⁰³ See also Dara Hallinan’s contribution on Germany.

³⁰⁴ Contribution for Slovakia.

³⁰⁵ Article 100(2) of the proposal for the new Personal Data Protection Act (*ZVOP-2*). The list includes: 1. The title of the project, 2. Detailed contact data of the researchers involved, 3. The field of study, 4. The goals and objectives, 5. Data management plan, 6. Categories and types of personal data required, 7. Whether data should be transmitted raw, pseudonymised, de-identified or anonymised, 8. Necessity of using already collected personal data, and disproportionate effort if new data would have to be collected (necessity and appropriateness), 9. Benefits resulting from the research outweigh any potential drawbacks to data subjects (proportionality), 10. Results publication strategy, 11. Comply with field-specific research ethics, if applicable, and 12. Who has access to data.

³⁰⁶ UK Health Research Authority, ‘Safeguards’ [webpage], last updated in 2018.

³⁰⁷ See Dara Hallinan’s contribution to this study.

³⁰⁸ Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, 0829/14/EN, WP 216, 10 April 2014, p. 9.

³⁰⁹ See e.g. Article 29 WP Opinion 05/2014 (absolute approach) vs CJEU, C-582-14, *Patrick Breyer v. Bundesrepublik Deutschland*, which seems to go into the relative approach direction. See also e.g., Spindler, G., Schmechel, P., ‘Personal Data and Encryption in the European General Data Protection Regulation’, *Journal of Intellectual Property, Information Technology and E-Commerce Law*, Vol. 7, No. 2, 2016, p. 163-177.

³¹⁰ Ienca, M., et al., 2019.

³¹¹ Bulgaria, Croatia, Cyprus, Germany, Greece, Hungary, Italy, Latvia, Romania, Slovakia, Slovenia, UK, and Norway

³¹² See the national contribution for Belgium in this study.

³¹³ ISC Intelligence in Science Input Paper.



**Coordinated
Supervision
Committee**



Work Programme 2025-2026

Adopted on 06.02.2025

Work Programme 2025-2026

Contents

1. INTRODUCTION.....	3
2. WORKING METHODS.....	5
3. Planned activities.....	5
3.1. Cross-cutting issues	6
3.2. Borders, Asylum and Migration.....	6
3.3. Police and Justice Cooperation	9
3.4. Digital Single Market.....	10

1. INTRODUCTION

The Coordinated Supervision Committee (hereinafter: CSC) hereby presents its third work programme for the biennium 2025-2026.

The CSC started its activities in 2019. Regulation 1725/2018 made the cooperation between the European Data Protection Supervisor and the national supervisory authorities, each acting within the scope of their respective competences, an obligation with the view of ensuring effective supervision of large-scale IT systems and of Union bodies, offices and agencies, where expressly provided for in the respective Union act. The CSC was initially entrusted with the coordinated supervision of the European Union Agency for Criminal Justice Cooperation (hereinafter: Eurojust) and the Internal Market Information (hereinafter: IMI).

This mandate has grown significantly over the years both in the fields of Police and Judicial Cooperation and of Borders, Migration and Asylum. The CSC has progressively taken over the coordinated supervision of the European Union Agency for Law Enforcement Cooperation (hereinafter: Europol), Schengen Information System (hereinafter: SIS) and Visa Information System (hereinafter: VIS), previously entrusted to the former Europol Cooperation Board and the respective Supervision Coordinated Groups.

The CSC also provides a forum for cooperation in the context of the supervision of the European Public Prosecutor's Office (hereinafter: EPPO), the Custom Information System established under Council Decision 2009/917/JHA (hereinafter :CIS JHA) and in the context of the supervision of personal data processing activities covered by Regulation (EU) 2023/2854 ("Data Act"), Regulation (EU) 2023/1773 on the carbon border adjustment mechanism transitional registry and Commission Implementing Regulation 2024/3084 establishing an Information System to facilitate the transfer of information between Member States competent authorities, and customs authorities related to deforestation and forest degradation.

The CSC has also been preparing for the coordinated supervision of the new Union's large-scale IT systems in the field of borders, visa, police and judicial cooperation, asylum and migration (LSITS)¹ and the framework for their interoperability between the (JHA Interoperability framework), which introduces a new approach to the management of data for borders and security. As LSITS become interconnected, it will be possible to simultaneously query all the LSITS as well as Europol data and Interpol databases, carry out biometric searches to cross-match biometric data present in all the LSITS, through one shared Biometric Matching Service (sBMS)², to have an individual file for each person that is registered in the Entry Exit System (hereinafter: EES), VIS, European Travel Information and Authorisation System (hereinafter :ETIAS), European Asylum Dactyloscopy Database (hereinafter: Eurodac) or the European Criminal Records Information System - Third Country Nationals (hereinafter :ECRIS-TCN in the Common Identity Repository (CIR)³ for the purpose of facilitating and assisting in

¹ Systems participating in the interoperability framework: the Schengen Information System (SIS); the Visa Information System (VIS); Eurodac; the Entry/Exit System (EES); the European Travel Information and Authorisation System (ETIAS); the European Criminal Record Information System for third country nationals (ECRIS TCN System).

² Art. 12 of Regulation (EU) 2018/817.

³ Art. 17 of Regulation (EU) 2018/817.

the correct identification of persons registered and to detect multiple identities of individuals by comparing data stored across different systems via the Multiple Identity Detector (MID)⁴.

The interconnection of LSITS will exponentially increase data flows and magnify the risks to data subjects generated by the operation of the underlying systems. Without specific measures in place, it will become extremely complex for data subjects to exercise their rights. Another set of challenges arises with regard to ensuring data quality and how to remove outdated/erroneous data from the databases when data flows so easily, on how to effectively inform all data recipients when data must be updated or is due to be erased, or the use of AI components or screening rules leading to profiling and automated-decision making.

The current Work Programme takes stock of this new broadened mandate and the need to ensure a high level of protection of the rights and freedoms of persons concerned by putting in place a meaningful coordinated supervision in the field of Borders, Migration and Asylum. It is expected that during the period of validity of this Work Programme at least two new EU LSITS (EES and ETIAS) will become operational, which will also mean the start of operations of the JHA Interoperability framework. The CSC will also be tasked with the coordinated supervision of EURODAC. A new advisory board, the VIS Fundamental Rights Guidance Board, will be created, for which the EDPB will have to nominate a representative and an alternate.

Under the previous Work Programme, substantial work had been dedicated to the preparation of the supervision of ETIAS, with the CSC participating as a member to the ETIAS Fundamental Rights Guidance Board and the creation of a dedicated Working Group on ETIAS. Two other working Groups have been created to coordinate actions vis-à-vis EES and VIS. Under this Work Programme, the CSC has decided to focus on ensuring that data subjects are provided with sufficient and adequate information about the functioning of this new ecosystem, on clarifying the allocation of roles (controller, joint controller, processor) in the systems falling under the JHA interoperability framework in order to avoid gaps in accountability and on streamlining cooperation when handling complaints filed by the data subjects.

In the field of Police and Judicial Cooperation, the CSC will consolidate the work conducted under the previous Work Programme and look at new issues stemming from the entry into force of new legal framework such as the Europol Regulation which now allows Europol and Member States to conduct joint operational analysis or the SIS Regulation which have introduced a new type of alert.

Finally the CSC will continue the coordinated supervision of IMI and will prepare for the new competences assigned to it under Regulation (EU) 2023/2854 (Data Act), Regulation (EU) 2023/1773 on the carbon border adjustment mechanism transitional registry and Commission implementing regulation 2024/3084 related to deforestation and forest degradation.

The CSC is also committed to improve its dialogue with stakeholders, in particular with NGOs, academia and researchers working in this field, by promoting reflection and debate on issues of common interest. Transparency is a guiding principle to our work and the CSC will use its revamped website more frequently within the European Data Protection Board (EDPB), to communicate with the public.

⁴ Art. 25 of Regulation (EU) 2018/817.

2. WORKING METHODS

In light of the extension of the mandate of the CSC and the vast amount of areas being covered by the coordinated supervision (1) Borders, Asylum and Migration, 2) Police and Judicial Cooperation, and 3) Digital Internal Market), the CSC has decided to reflect on its working methods to ensure the efficiency of the coordinated supervision and more flexibility and reactivity in the way how the CSC operates.

The experience of the CSC has shown that it is not always possible to ensure the participation of all supervisory authorities (SAs) in all work streams, in particular when the CSC is asked to react swiftly or to participate in external meetings, which require prior coordination of CSC members. The lack of resources attributed to the SAs as well as the CSC Secretariat also slows down the work of the CSC.

In addition to the possibility of having drafting teams, the CSC is considering to organise the work on the different streams with the creation of ad hoc Working Groups. While drafting teams are responsible for the elaboration of documents to be approved by the CSC, the mandate of the Working Groups would be broader. The CSC decides on the creation of a Working Group when there is a need to follow-up more closely the coordinated supervision of a thematic area.

This new working method has emerged from practical experience. In 2024, the CSC created two ad hoc Working Groups: one dedicated to the preparation of the coordinated supervision of ETIAS and one dedicated to the preparation of the coordinated supervision of EES. It was also decided to create a third Working Group dedicated to the coordinated supervision of VIS. Each of them gathered a subset of SAs which had decided to allocate specific resources to the preparation of the supervision of these systems.

Taking into account that it is not possible for all SAs to participate in all Working Groups, because of a shortage of resources, for the next reporting period, the CSC will work in Plenaries (four per year), where all SAs are represented and decisions are made as well as in Working Groups, where only a subset of SAs actively contribute. This will allow CSC members to focus their resources on their own priorities and to pool knowledge and expertise to ensure an effective coordinated supervision. Knowledge sharing thus becomes a key task for the Working Groups.

The creation of Working Groups does not preclude the work in Drafting Teams.

3. PLANNED ACTIVITIES

The CSC's mandate covers three different areas: 1) Borders, Asylum and Migration, 2) Police and Judicial Cooperation and 3) Digital Single Market. Each of these areas entails specific challenges and concerns with regard to data protection and is tackled separately by the CSC. The CSC will however work on two cross-cutting issues, the clarification of allocation of roles as a necessary requirement to avoid any accountability gap and the streamlining of cooperation in the handling of complaints in order to uphold data subjects' rights.

The planned activities in each of these areas take into account the tasks assigned to it under Art. 62 EUDPR and respective specific Regulations:

- Ensure that data subjects are able to exercise their rights;

- Promote the exchange of information and joint audits or coordinated inspections by national SAs and the EDPS;
- Reach a common understanding between its participating authorities on their respective scope of supervision, applicable legal basis, and the areas where they need to cooperate and coordinate;
- Prepare the CSC's work on the supervision of the EU bodies and information systems that will fall within the CSC's remit in the coming years.

The CSC will be flexible and work on other activities that may not be included in this work programme but that participating authorities or Working Groups may bring to its attention, based on their relevance, urgency or unforeseen character.

3.1. Cross-cutting issues

As systems become interoperable and EU Agencies active in the field of the Area of Freedom, Security and Justice are encouraged to increase information sharing, including personal data, between themselves and with national authorities, the CSC has identified some cross-cutting topics that require closer attention to avoid any gap in the protection afforded by the data protection framework and ensure a high level of protection of data subjects' rights:

- **Clarifying the allocation of roles (controller, joint controller, processor) in the systems falling under the JHA Interoperability framework.** The role of different authorities involved in the different systems forming the JHA Interoperability framework (such as ETIAS or VIS) is not always clarified by the legal framework or correctly reflected in their implementation, leading to a situation where some authorities are categorised as processors, despite their clear role as controllers or joint controllers. A similar situation has been observed in the context of the Europol Regulation in the context of "joint operational analysis" introduced by Art. 20a of the latest amendment of the Europol Regulation, or where Member States' police and/or Europol perform 'joint' operational analysis using a Member State or third country (e.g. U.S.) environment. There is thus a need to clarify the allocation of roles in order to ensure both legal certainty and accountability from all the national authorities and EU Agencies and bodies involved.
- **Streamlining cooperation when handling complaints (JHA Interoperability framework and Europol, Eurojust, EPPO).** An efficient and smooth handling of complaints from data subjects will be one of the main challenges that SAs and the EDPS will face when the JHA Interoperability framework starts operating, due to the large amount of authorities involved in the processing at stake, all subject to different legal frameworks and SAs. The CSC will build on the experience in the handling of Europol's complaints in order to streamline its cooperation.

3.2. Borders, Asylum and Migration

One of the most prominent challenges for the CSC is to adequately ensure the coordinated supervision of the JHA Interoperability framework, due to the number of EU LSITS and authorities involved in the

framework. The CSC can benefit from the experience of its members in the coordinated supervision of SIS or VIS, but is also faced with the challenges of ensuring the coordinated supervision of the interoperability of EU-LSITS, with new systems and new functionalities, such as the use of screening rules both in ETIAS and VIS, which will have a high impact on data subjects' rights and freedoms. To that end, three ad hoc Working Groups have already been created, one with a focus on ETIAS, another with a focus on EES and the third on VIS, in order to ensure a timely consideration of potential data protection concerns that might arise in the setting-up and running of these systems.

This is accompanied by a series of reporting obligations with regard to the activities conducted in respect of the following:

- On a yearly basis, coordinated supervision over SIS (together with the obligation to collect from MS information on the exercise of data subject rights). The report should contain information provided by national competent authorities in Member States to the EDPB on the exercise of data subjects' rights, on court proceedings and on mutual recognition of final decisions to be included in the joint report of activities regarding the Schengen Information System as per Article 54(3) of Regulation (EU) 2018/1861 and Article 68(3) of Regulation (EU) 2018/1862.
- Every two years for EES, ETIAS, the interoperability components and Prüm II when the operations start. The joint reports should be provided to the European Parliament, the Council, the Commission, eu-LISA (for EES, ETIAS, Interoperability Regulations), to Frontex (ETIAS, Interoperability Regulations) and to Europol (Interoperability Regulation in the field of borders and visa and in the field of police and judicial cooperation, asylum and migration)⁵.

Promote and facilitate the exercise of data subjects' rights

- Coordinate on EES and SIS information campaigns.
- Work on the support of the exercise of rights vis-à-vis the different information systems, as a roadmap for data subjects to navigate among systems, controllers, formalities for submission, deadlines for replies, and so forth - in particular EES and ETIAS.

Actions specific to certain systems

SCHENGEN INFORMATION SYSTEM (SIS)

- Legal interpretation of the timeframe set in Art 55(2) of the Regulation (EU) 2018/1861 and Art 69(2) of the Regulation (EU) 2018/1862.

⁵ Pursuant Article 57(4) of Regulation (EU) 2017/2226 for EES, Article 68(4) of Regulation (EU) 2018/1240 for ETIAS, Article 61(3) of Regulation (EU) 2024/982 for Prüm II, Article 53(3) of Regulation (EU) 2019/817 for the interoperability in the field of borders and visa and Article 53(3) of Regulation (EU) 2019/818 for the interoperability in the field of police and judicial cooperation, asylum and migration.

- Monitoring of Art. 40 alerts (SIS Regulation 2018/1862).
- Obligation to check logs of Art. 12 SIS Regulations.
- Monitoring the implementation of the provisions on “information alerts” to be inserted in the SIS by Member States on proposal by Europol, either at national level (SIS) or/and at EU level (Europol), in particular by checking the periodic reporting mechanism in place on those alerts.
- Ensure the participation of SAs in training and joint evaluation missions in relation to the SIS in the framework of Schengen evaluation and monitoring mechanism (SCHEVAL).

EUROPEAN TRAVEL INFORMATION AND AUTHORISATION SYSTEM (ETIAS)

- Participation as a member to the ETIAS Fundamental Rights Guidance Board.

VISA INFORMATION SYSTEM (VIS)

- Ensure the participation of SAs in training and joint evaluation missions in relation to the VIS in the framework of Scheval evaluation mechanism.
- Prepare for the participation as a member to the VIS Fundamental Rights Guidance Board.

Prepare the coordinated supervision of new systems

The CSC will carry out the following tasks under this activity:

- Monitor developments and share information on the entry into operation of reforms of existing EU information systems and agencies or creation of new ones.
- Prepare the CSC’s assumption of the coordinate supervision over the EU information systems that will fall within the scope of the CSC (EURODAC):
 - Take stock of the relevant undergoing activities of the existing supervision coordination groups.
 - Engage with those groups on specific EU information systems and agencies and with the EDPS, which provides their secretariat, to prepare their transition to the coordinated supervision of the CSC.

3.3. Police and Judicial Cooperation

In the area of police and judicial cooperation, the CSC deals with the EU institutions (EUIs) Europol, Eurojust and the EPPO, as well as with the data processing operations covered by the Prüm-II-Regulation.

The focus in this area is the promotion and facilitation of the exercise of data subjects' rights, the examination of difficulties in the interpretation of the underlying law and the support of joint actions, in particular fact-finding or inspections. Being one central challenge with the ever more complex processing activities within and across EUIs/systems, the CSC aims to support its members actively in clarifying the roles of the respective actors being controllers, joint controllers or processors.

In addition, the CSC in its activity aims to tackle the cross-cutting nature of many of the processing operations, as they either may directly involve two or more EUIs or systems, or indirectly affect two or more, e.g. by way of providing information that are then being used for the purpose of another EUI/system.

EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT COOPERATION (EUROPOL)

- Joint inspections on matters identified on a systematic and fact-based approach.
- Coordinated examination of how Single Point of Contacts (SPOCs) are being set up in each of the Member States. These SPOCs are to be established following national transposition of the Directive 2023/997 (Information Exchange Directive). The deadline for transposition is 12 December 2024 and it has currently been transposed by FR and RO. As there is no direct reference to coordinated supervision in the Information Exchange Directive, this item would focus on the sharing of information by SPOCs with Europol.
- Streamlining procedures for joint investigations and safeguarding a common approach as regards the setting-up of the SPOCs when transposing the Information Exchange Directive into national law by the end of 2024.
- Collect and exchange information on the technical implementation of communication systems of exchange of personal data for law enforcement purposes (e.g. SIENA).
- Inspecting the lawfulness of processing of data on minors sent by national competent authorities to Europol as regards national law and the Europol Regulation, based on prior EDPS referrals and involving the SAs of those MS concerned.
- Streamlined procedures for handling of Europol complaints, indirect access, joint actions etc. between national SAs and the EDPS and access requests from citizens
- Monitoring the implementation of the provisions of "information alerts" to be inserted in the SIS by Member States on proposal by Europol, either at national level (SIS) and/or at EU level (Europol), in particular by checking the periodic reporting mechanism in place on those alerts.
- Joint controllership of Europol and the competent authorities of the Member States in joint operational analysis cases, e.g. under Art. 20a of the Europol Regulation, or where Member

States police and/or Europol perform 'joint' operational analysis using a Member State or third country (e.g. U.S.) environment.

- Keeping up to date the guide on the right of access for Europol.

EUROPEAN UNION AGENCY FOR CRIMINAL JUSTICE COOPERATION (EUROJUST)

- Assess the participation of third country authorities in Joint Investigation Teams under the Eurojust scope and support.
- Examine the data quality issues related to data inserted in the Eurojust Counter-Terrorism Register and possibly coordinate a supervisory action at national level on the issue.
- Survey on SAs independence, powers and legal tasks in relation to police and judicial cooperation in criminal matters.
- Draft new guide on the right of access regarding Eurojust.

EUROPEAN PUBLIC PROSECUTOR'S OFFICE (EPPO)

- Keep monitoring the implementation of the EPPO offices at Member State level and the interplay between EPPO and the national databases.
- Studying the interplay between EU and national law and its application to the activities of supervisors at EU and national level reaching understandings on their respective areas of supervision.
- Draft new guide on the right of access regarding the EPPO.

PRUM II

- Follow state-of play of implementation.
- Support members in taking up supervision, including by joint fact-finding actions.

3.4. Digital Single Market

In the area of Digital Single Market, the CSC deals with Internal Market Information System (IMI).

The focus in this area lies on continuing to safeguard data subjects' rights, but also on the proper technical implementation of the systems with a focus on the handling of user and access rights.

- Follow-up on the coordinated fact-finding action on how national competent authorities exercise their obligations concerning IMI on management of users' access to the information system.
- Assess the allocation of roles in terms of controllership within the IMI in relation to the data processed.
- Evaluate the compliance with the IMI transparency obligations and recommendations on handling data subject requests (follow-up to actions conducted under the work programme 2022-2024).
- Possible further joint inspections on matters identified on a systematic and fact-based approach.

3.5. Preparing for new competences

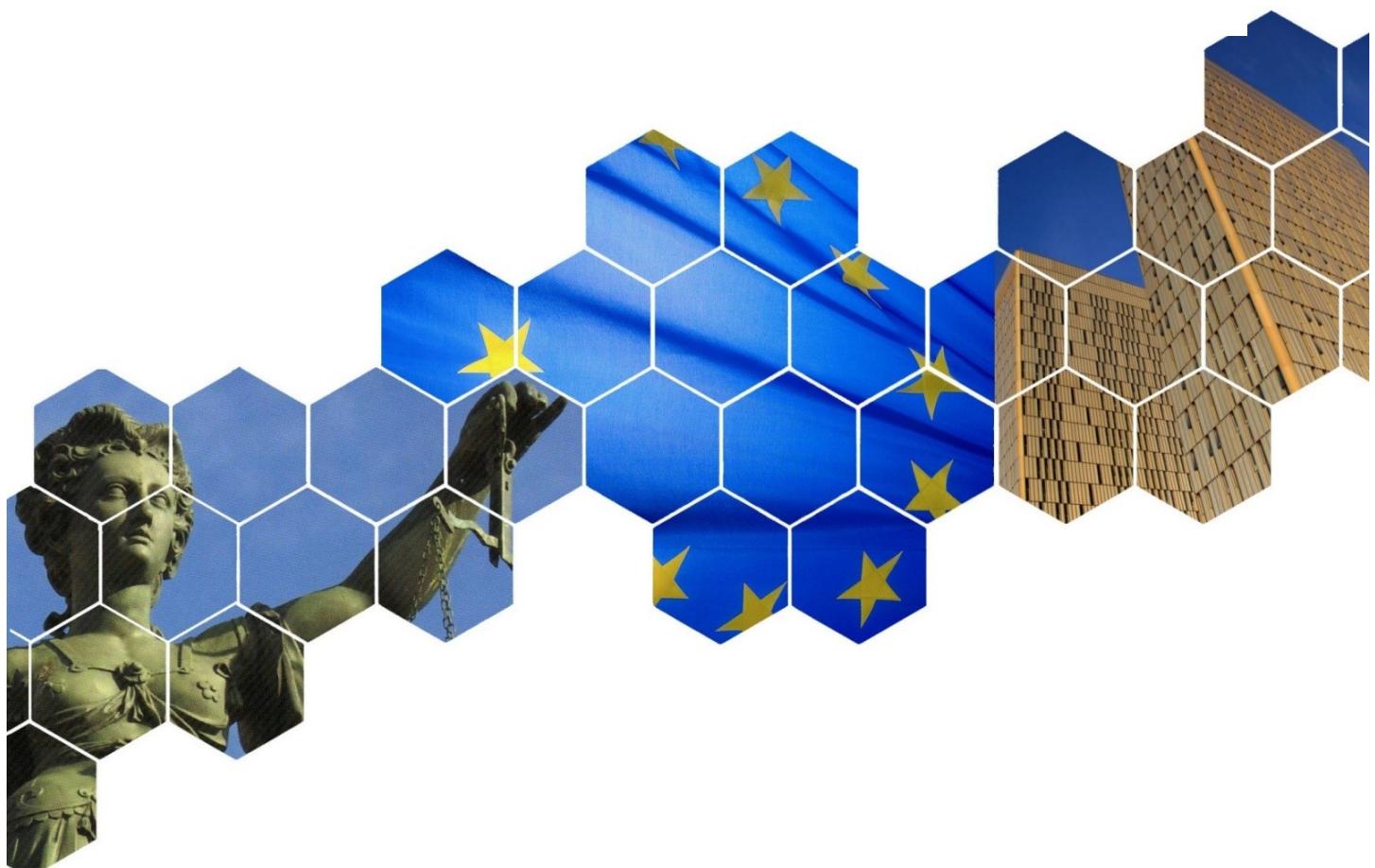
The CSC will prepare for the assumption of new competences assigned to it under three new EU legal instruments:

- **Regulation (EU) 2023/2854 ("Data Act").** The Data Act establishes rules for accessing and using data within the European data economy. Article 37(3) entrusts the supervision of personal data processing covered by the Regulation to national SAs, the EDPS insofar as it concerns the Commission, the European Central Bank or Union bodies and refers to Article 62 EUDPR as mechanisms for coordinated supervision. The Data Act entered into force on 11 January 2024, and it will become applicable in September 2025.
- **Regulation (EU) 2023/1773 on the carbon border adjustment mechanism transitional registry.** The Regulation lays down reporting obligations for the purposes of carbon border adjustment mechanism. Article 33(2) refers to Article 62 EUDPR as mechanism to ensure coordinated supervision between SAs and the EDPS for the processing of personal data registered in the carbon border adjustment mechanism transitional Registry and the components of electronic systems developed at national level.
- **Commission Implementing Regulation 2024/3084 related to deforestation and forest degradation.** It lays down the rules for the functioning of the Information System, including rules for the protection of personal data and exchange of data with other IT systems. Regulation (EU) 2023/1115 lays down rules to minimise the Union's contribution to deforestation and forest degradation. It does this by imposing due diligence obligations on operators and traders placing on, making available on, or exporting from the Union market certain commodities and products. It also establishes the creation of an Information System and provide access to it to operators and traders, and if applicable, their authorised representatives, competent authorities, and customs authorities, to implement their respective obligations. The Information System should facilitate the transfer of information between Member States competent authorities, and customs authorities. Article 12(7) refers to Article 62 EUDPR as coordinated supervision mechanism between the SAs and the EDPS. Regulation (EU) 2023/1115 is in force since December 2024.

Study on the national administrative rules impacting the cooperation duties for the national supervisory authorities

Final Report

EDPS/2019/02-07



August 2020

This study has been prepared by Milieu under Contract No EDPS/2019/02-07 for the benefit of the EDPB.



The study has been carried out by a team of researchers from Milieu, University of Namur (CRIDS), Vrije Universiteit Amsterdam (CLI) and Leiden University (eLaw). The leading author of the study report is Jean Herve (CRIDS).

The information and views set out in this study are those of the author(s) and do not necessarily reflect the official opinion of the EDPB. The EDPB does not guarantee the accuracy of the data included in this study. Neither the EDPB nor any person acting on the EDPB's behalf may be held responsible for the use which may be made of the information contained therein.

Milieu Consulting SRL, Chaussée de Charleroi 112, B-1060 Brussels, tel.: +32 2 506 1000; e-mail: EDPB.legalstudies@milieu.be; web address: www.milieu.be.

Study on the national administrative rules impacting the cooperation duties for the national supervisory authorities

TABLE OF CONTENTS

ABSTRACT	5
EXECUTIVE SUMMARY	6
1 INTRODUCTION	8
1.1 Objectives of the study	8
1.2 Scope of the study.....	9
1.3 Methodology of the study	9
1.3.1 Research methods for task 1: desk research and creating a table	9
1.3.2 Research methods for tasks 2, 3 and 4.....	10
1.4 Structure of the study	10
2 NATIONAL ADMINISTRATIVE RULES IMPOSING DEADLINES IMPACTING THE MOMENT ON WHICH THE DRAFT DECISION HAS TO BE SHARED WITH A CSA	11
2.1 Overview of national administrative rules imposing deadlines impacting the moment when the draft decision has to be shared with a CSA	11
2.2 General trends observed in relation to the national administrative rules imposing deadlines impacting the moment when the draft decision has to be shared with CSAs	14
2.3 Questions & Challenges to cooperation duties stemming from the application of national administrative rules imposing deadlines impacting the moment when the draft decision has to be shared with CSAs	14
2.4 Suggestions and possible solutions	15
3 NATIONAL ADMINISTRATIVE RULES REGARDING THE ADMISSIBILITY OF COMPLAINTS FROM INDIVIDUALS	16
3.1 Overview of national administrative rules regarding the admissibility of complaints from individual	16
3.2 General trends observed in relation to the national administrative rules regarding the admissibility of complaints from individuals	18
3.3 Questions & challenges to cooperation duties stemming from the application of national administrative rules regarding the admissibility of complaints from individuals.....	19
3.4 Suggestions and possible solutions	19
4 NATIONAL ADMINISTRATIVE RULES ON THE RIGHT TO BE HEARD	21
4.1 Overview of national administrative rules on the right to be heard.....	21
4.2 General trends observed in relation to the national administrative rules on the right to be heard.....	22
4.3 Questions & challenges to cooperation duties stemming from the application of national administrative rules on the right to be heard.....	23
4.4 Suggestions and possible solutions	23
5 NATIONAL ADMINISTRATIVE RULES ON AMICABLE SETTLEMENTS	25
5.1 Overview of national administrative rules on amicable settlements	25
5.2 General trends observed in relation to the national administrative rules on amicable settlements	26
5.3 Questions & challenges to cooperation duties stemming from the application of national administrative rules on amicable settlements	27
5.4 Suggestions and possible solutions	27

6 NATIONAL ADMINISTRATIVE RULES ON THE PRIOR NOTIFICATION OF FORTHCOMING INVESTIGATIONS OR EXERCISE OF CORRECTIVE POWERS	28
6.1 Overview of national administrative rules on the prior notification of forthcoming investigations or exercise of corrective powers.....	28
6.2 General trends observed in relation to the national administrative rules on the prior notification of forthcoming investigations or exercise of corrective powers	30
6.3 Questions & challenges to cooperation duties stemming from the application of national administrative rules on the prior notification of forthcoming investigations or exercise of corrective powers.....	31
6.4 Suggestions and possible solutions	31
7 NATIONAL ADMINISTRATIVE RULES IMPOSING STEPS OR DECISIONS PERTAINING TO THE OSS PROCEDURE	32
7.1 Overview of national administrative rules imposing steps or decisions pertaining to the OSS procedure	32
7.2 General trends observed in relation to the national administrative rules imposing steps or decisions pertaining for the OSS procedure	36
7.3 Questions & challenges to cooperation duties stemming from the application of national administrative rules imposing steps or decisions to the OSS procedure.....	38
7.4 Suggestions and possible solutions	38
8 CONCLUSION.....	39
ANNEX 1 – QUESTIONNAIRE FOR THE NATIONAL SUPERVISORY AUTHORITIES	41
ANNEX 2 – LIST OF STAKEHOLDERS CONTACTED.....	43
ANNEX 3 – SOURCES OF INFORMATION.....	44
ANNEX 4 - ACRONYMS AND ABBREVIATIONS	50

LIST OF TABLES

Table 1: Overview of NARs imposing deadlines impacting the moment when the draft decision has to be shared with the CSAs	11
Table 2: Overview of NARs regarding the admissibility of complaints from individuals	16
Table 3: Overview of NARs on the right to be heard	21
Table 4: Overview of NARs regarding rules on amicable settlements	25
Table 5: Overview of NATs on the prior notification of forthcoming investigations or exercise of corrective powers.....	28
Table 6: Overview of NARs imposing steps or decisions pertaining to the OSS procedure	32
Table 7: List of competent SAs	43
Table 8: Overview of national laws	45
Table 9: Acronyms and abbreviations	50

ABSTRACT

This study analyses the national administrative rules applicable when the national supervisory authorities (SA) carry out their cooperation duties in the context of a One-Stop-Shop (OSS) procedure.

It provides an overview of the national administrative rules applicable to SAs when they carry out their cooperation duties and to identify their specificities, which could raise questions or challenges to the completion of their GDPR cooperation duties in the context of an OSS procedure, with respect to the following six issues:

- deadlines impacting the moment on which draft decisions should be shared with SAs;
- the admissibility of complaints from individuals;
- the right to be heard;
- amicable settlements;
- the prior notification of forthcoming investigations or exercise of corrective powers;
- steps or decisions pertaining to the OSS procedure.

On this basis the study points out the main questions and challenges to cooperation duties stemming from these national administrative rules.

Based on its findings, the study offers suggestions or solutions for each of the six topics covered by the analysis, before suggesting a more global solution consisting of assessing the possibility of drafting Recommendations or Guidelines at European level (EDPB) specifying how to conduct an OSS procedure (starting with the identification of cross-border processing, then with the investigation phase, the information and consultation of the SAs, the notification and hearing of the parties, the decision-making procedure, and the legal effects of the decisions adopted during the OSS procedure).

EXECUTIVE SUMMARY

I. Overview of the national administrative rules and their specificities regarding cooperation duties

The report offers six tables providing an overview of the national administrative rules and their specificities regarding cooperation duties in the context of an OSS procedure for each of the six topics covered by the study.

II. General trends observed in relation to national administrative rules which have an impact on cooperation duties

In addition to the rules laid down in the GDPR, all SAs have to comply with national general administrative rules when carrying out their cooperation duties in an OSS procedure. In addition, a large majority of countries have passed some specific rules regarding the way their cooperation duties should be organised in OSS procedures. A minority of countries have passed more comprehensive national administrative rules regarding the OSS mechanism.

A vast majority of countries recognise the controllers' and processors' fundamental right to be heard. They also recognise, to some extent, the obligation to provide information to the complainant and/or the controller or processor.

In a large majority of countries, complaints must comply with requirements laid down by national administrative rules.

In nearly all the countries, time limits or deadlines are suspended, or may be extended, in case of an OSS procedure.

A substantial number of countries recognise the possibility of amicable settlements between the complainant and the controller or processor.

Finally, there is no harmonisation regarding the steps leading to a decision in the context of an OSS procedure.

III. Main challenges in relation to the application of the national administrative rules on cooperation duties

Deadlines are not the same in all the countries (in terms of legal nature and legal effects) and there is no coherence as to the moment when draft decisions should be shared with competent supervisory authorities (CSAs).

The requirements for the admissibility of the complaints from individuals vary considerably from one country to another, either in terms of nature or in terms of content.

The right to be heard exists, to some extent, in 25 countries. However, there is no harmonisation as to who should be heard nor as to the moment when parties should be heard.

The possibility to reach an amicable settlement between controllers or processors and complainants does not exist in all countries. There might be controversy on whether amicable settlements are possible for cross-border cases with an impact broader than just locally. Where amicable settlements are reached, there is no clear indication on their impact on the OSS procedure.

There is no convergence regarding the prior notification of forthcoming investigations or exercise of corrective powers. It is an obligation in some countries and not in others.

The procedure applied when handling an OSS case varies from country to country.

IV. Suggestions and possible solutions

The study offers suggestions or solutions for each of the six topics covered by the analysis in order to consolidate the operational framework of the OSS mechanism. It also suggests a more global solution consisting of assessing the possibility to draft Recommendations or Guidelines at European level (EDPB) specifying how to conduct an OSS procedure (starting with the identification of cross-border processing, then with the investigation phase, the information and consultation of the SAs, the

notification and hearing of the parties, the decision-making procedure, and the legal effects of the decisions adopted during the OSS procedure).

1 INTRODUCTION

From among the provisions relating to cooperation duties, the General Data Protection Regulation (GDPR¹) first regulates cooperation between the lead supervisory authority (LSA) and the competent supervisory authorities (CSAs) in the context of the one-stop-shop (OSS) mechanism (cf. Article 60 of the GDPR), as follows:

1. the LSA must cooperate with CSAs;
2. the LSA and CSAs must exchange all relevant information with each other; and
3. the LSA may request at any time other CSAs to provide mutual assistance.

The LSA must, immediately, communicate the relevant information to the other CSAs.

The LSA should also (and without any delay) submit a draft decision to the CSAs for their opinion and it should take due account of their views (cf. Article 60(3)-(7) of the GDPR).

The LSA and the CSAs will supply the information to each other by electronic means, using a standardised format (e.g. cf. Article 60(12) of the GDPR).

The GDPR also provides for rules on the mutual assistance between supervisory authorities (SAs), which covers, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations (cf. Article 61(1) and (2) of the GDPR).

SAs may also conduct joint operations including joint investigations and joint enforcement measures in which members or staff of the SAs of other Member States are involved (cf. Article 62 of the GDPR).

This study focuses on the **national administrative rules** (either national data protection rules or national general administrative rules) applicable to the SAs' activities when carrying out their cooperation duties in the context of an **OSS procedure**.

1.1 OBJECTIVES OF THE STUDY

The objectives of the study are outlined in the annex to the Contract.

The first objective of the study is to provide an overview of the national administrative rules that might be applicable when SAs are carrying out their cooperation duties and to identify their specificities which could raise questions or challenges to the completion of their GDPR cooperation duties in the context of an OSS procedure, e.g. with respect to the following six issues:

- whether the national systems impose deadlines impacting the moment when the draft decision will be shared with the other SAs concerned;
- whether the national systems impose the duty of addressing all complaints from individuals or only some of them (in addition to what is provided by Article 57(4) of the GDPR);
- whether the national system provides for duties on the right to be heard for the affected parties even before the consultation of the other SAs concerned on the draft decision;
- whether some national legislative systems enable the conclusion of amicable settlements with the controller or the processor and if yes, whether the latter would take place prior to the consultation of the other supervisory authorities concerned on the draft decision;
- whether some national legislative systems impose duties of prior notification of the controller/processor of any investigation or forthcoming exercise of corrective powers and

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, pp. 1–88, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593600370255&uri=CELEX:32016R0679>.

- whether the latter should take place prior to the consultation of the other supervisory authorities concerned on the draft decision;
- whether the national systems impose different steps or the adoption of different decisions relating to a case (i.e. investigation reports, decision on the exercise of corrective powers, decision on the publicity of the decision) and at which moment the other CSAs should be consulted, while taking into consideration Recital 129 in line with the GDPR.

The second objective of the study is to identify general trends in relation to the national systems.

The third objective of the study is to provide a legal analysis of how the national specificities could potentially raise questions or challenges in relation to the application of the GDPR cooperation duties in the context of an OSS procedure.

The fourth and last objective of the study is to provide suggestions on how to combine the national and European frameworks and on possible solutions, including legislative initiatives, taking into consideration the respective scope of competence between the EU and the Member States.

A separate task was designed around each of the objectives to make sure that each one was sufficiently covered.

1.2 SCOPE OF THE STUDY

The study covers the 27 Member States of the European Union and the three EFTA-EEA States. It analyses the national administrative rules that might be applicable to the SAs' activities when they are carrying out their cooperation duties in the context of an OSS procedure.

1.3 METHODOLOGY OF THE STUDY

1.3.1 Research methods for task 1: desk research and creating a table

To complete the first task, relating to the first study objective, the team first proceeded with the analysis of all the Member States' national laws passed to implement the GDPR, in search for information on the national administrative rules applicable to the SAs' activities when carrying out their cooperation duties in the context of an OSS procedure. The EDPB Secretariat provided the team with the English translation of these national laws. Due to the language capacity of the team, some national laws were also studied in native languages.

In addition, a questionnaire was drafted and sent to the SAs of all the Member States and three EFTA-EEA Members (cf. the model in annex 1). Such a questionnaire was seen as the most efficient way to get first-hand and reliable information on the national administrative rules, which might have an impact on the cooperation mechanism instituted by the GDPR in the context of an OSS procedure. The twenty questions were validated by the EDPB Secretariat, which then disseminated the questionnaire centrally. The response rate from the SAs was very high (29 out of 30).

The team also analysed the responses provided by the SAs to a questionnaire conducted by the European Commission in the context of the evaluation of the GDPR, the completion of which is foreseen by Article 97 of the GDPR. The team reviewed those responses that related to questions on Chapter VII of the GDPR. These results were provided to the team by the EDPB Secretariat. It is noted that the results are also publicly available on the EDPB's website.

The EDPB Secretariat also provided the team with the results from two of their internal questionnaires regarding "amicable settlements" and regarding the investigation of complaints (specifically on the sharing of information before submitting a draft decision).

The team then populated an overview table (an excel file) with all the information gathered from the aforementioned sources. Due to methodological constraints, the information provided from these sources has not been validated.

1.3.2 Research methods for tasks 2, 3 and 4

Tasks 2, 3 and 4, covering second, third and fourth study objectives, were completed based on desk research and legal analysis of the information gathered during task 1.

1.4 STRUCTURE OF THE STUDY

The study dedicates separate sections to each of the six issues outlined in connection with the first objective. These sections provide:

- An overview of the national administrative rules applicable to the issue in question (this overview takes the form of a table, which provides a snapshot of the pertaining national administrative rules. The last column of the table states whether these rules are set out in national legislation or else stem from the practices of the supervisory authorities);
- General trends observed in relation to the applicable national administrative rules;
- Questions and challenges raised by the national administrative rules;
- Suggestions and possible solutions to the questions and challenges identified.

2 NATIONAL ADMINISTRATIVE RULES IMPOSING DEADLINES IMPACTING THE MOMENT ON WHICH THE DRAFT DECISION HAS TO BE SHARED WITH A CSA

2.1 OVERVIEW OF NATIONAL ADMINISTRATIVE RULES IMPOSING DEADLINES IMPACTING THE MOMENT WHEN THE DRAFT DECISION HAS TO BE SHARED WITH A CSA

Table 1: Overview of NARs imposing deadlines impacting the moment when the draft decision has to be shared with the CSAs

Member State/EEA State	NARs imposing deadlines impacting the moment when the draft decision has to be shared with CSAs	Origin of the rule (national legislation or SA's practice or interpretation)
Austria	<ul style="list-style-type: none"> ▪ Six-month time-limit to handle complaints & investigate ▪ This time-limit is suspended in case of an OSS procedure ▪ Draft decision is shared when all necessary evidence has been gathered and all parties heard (when the case is ready for decision) 	<ul style="list-style-type: none"> ▪ National legislation: Art. 73 of the General administrative Procedure Act (GAPA) ▪ National legislation: Art. 24(10) of the Federal Act concerning the Protection of Personal Data (DSG) ▪ SA's practice
Belgium	<ul style="list-style-type: none"> ▪ 30-day deadline for the litigation chamber to ask for additional investigations to be carried out by the Inspection Service, from the day the litigation chamber has been seized by the front office ▪ Draft decision is shared when parties have submitted their first conclusions 	<ul style="list-style-type: none"> ▪ National legislation: Arts. 55-56 and 69, 96 of the 2017 Act ▪ SA's practice
Bulgaria	<ul style="list-style-type: none"> ▪ No exact moment when draft decisions should be shared 	<ul style="list-style-type: none"> ▪ No information
Croatia	<ul style="list-style-type: none"> ▪ 30 to 60-day deadline to process requests and inquiries ▪ No exact moment when draft decisions should be shared 	<ul style="list-style-type: none"> ▪ SA's practice ▪ No information
Cyprus	<ul style="list-style-type: none"> ▪ 30-day deadline to examine a complaint and provide the complainant with some information 	<ul style="list-style-type: none"> ▪ National legislation: subsect. (b) and (c) of Art. 24 of the Law 125(I)/2018
Czech Republic	<ul style="list-style-type: none"> ▪ 30 to 60-day deadline to issue a decision ▪ This deadline may be extended ▪ No exact moment when draft decisions should be shared 	<ul style="list-style-type: none"> ▪ National legislation: sect. 71(1) and 71(3) of the Administrative Procedural Code (APC) ▪ National legislation: Art. 80(4) of the APC ▪ No information
Denmark	<ul style="list-style-type: none"> ▪ No deadlines to proceed were indicated by the SA ▪ No exact moment when draft decisions should be shared (until now they did not need to share information before submitting a draft decision) 	No information
Estonia	<ul style="list-style-type: none"> ▪ 30 to 60-day deadline to handle and settle complaints ▪ This deadline may be extended to a reasonable period 	<ul style="list-style-type: none"> ▪ National legislation: Art. 61 of the Personal Data Protection Act (PDPA) ▪ National legislation: Art. 33(1), (5) and (6), and Art. 53(1) of the Code of Civil Procedure
Finland	<ul style="list-style-type: none"> ▪ There are time-limits set up by law 	<ul style="list-style-type: none"> ▪ National legislation: Arts. 18-21, 23, 23(A) and 24(5) of the 2018 Data Protection Act (DPA)

Member State/EEA State	NARs imposing deadlines impacting the moment when the draft decision has to be shared with CSAs	Origin of the rule (national legislation or SA's practice or interpretation)
	<ul style="list-style-type: none"> ▪ A case should be considered without undue delay ▪ No exact moment when draft decisions should be shared; the SA considers that it should be shared once the fact finding and legal analysis are finalised and the decision has been taken by the SA, therefore enabling other SAs to express relevant and reasoned objections 	<ul style="list-style-type: none"> ▪ SA's practice ▪ SA's practice
France	<ul style="list-style-type: none"> ▪ No deadlines for handling complaints but three months of silence implies rejection of the complaint ▪ Draft decision from the Chair is shared as soon as it is adopted ▪ Draft decision from the restricted committee is shared after the hearing of data controller (DC) and/or data processor (DP) 	<ul style="list-style-type: none"> ▪ SA's practice and interpretation ▪ SA's practice and interpretation ▪ SA's practice and interpretation
Germany	<ul style="list-style-type: none"> ▪ No deadlines other than those set up by the GDPR ▪ No exact moment when the draft decision should be shared 	No information
Greece	<ul style="list-style-type: none"> ▪ No deadlines nor timeline ▪ The draft decision is shared with CSA after its approval by the College of Commissioners of the HDPA 	<ul style="list-style-type: none"> ▪ SA's practice ▪ SA's practice
Hungary	<ul style="list-style-type: none"> ▪ In Hungary there is no regulation that prescribes when the draft decision has to be shared with the CSAs. ▪ However the Hungarian DPA has the following deadlines for its procedures: Two-month deadline for inquiry and 150 days for the authority procedure. The deadline for the authority procedure is suspended when performing cooperation duties ▪ Information is shared with other SAs when necessary before submitting the draft decision 	<ul style="list-style-type: none"> ▪ National legislation: Art. 55(1) of the 2011 Act CXII for inquiry, and Art 60/A (1) for authority procedure ▪ SA's practice
Iceland	<ul style="list-style-type: none"> ▪ No deadlines but cases should be handled quickly 	<ul style="list-style-type: none"> ▪ National legislation: Art. 9 of the Administrative Procedures Act (APA)
Ireland	<ul style="list-style-type: none"> ▪ No deadline nor timeline to handle a complaint or an investigation ▪ Information is shared from the beginning of the inquiry ▪ Draft decision is notified as soon as it is issued: the SA will share a draft decision with the other supervisory authorities concerned once the inquiry stage is complete and the respondent concerned has had the opportunity to be heard in relation to the decision-maker's draft decision. Circulating the draft decision at this point in time further ensures that the respondent has been afforded their fair procedural rights, pursuant to the Irish common law 	<ul style="list-style-type: none"> ▪ No information ▪ SA's practice ▪ SA's practice and interpretation of Sections 111 and 113 of the 2018 Act
Italy	<ul style="list-style-type: none"> ▪ Nine to twelve-month deadline for handling a complaint ▪ The time limit is suspended during an OSS procedure ▪ The draft decision is prepared after collecting CSAs opinions and it is shared after its approval by the Garante 	<ul style="list-style-type: none"> ▪ National legislation: Art. 143(3) of the Italian Data Protection Code (IDPC) ▪ National legislation: Art. 143(3) of the Italian Data Protection Code (IDPC) ▪ SA's practice
Latvia	<ul style="list-style-type: none"> ▪ One to four-month deadline to answer a complaint 	<ul style="list-style-type: none"> ▪ National legislation: cf. Administrative Procedure Law (APL)
Liechtenstein	<ul style="list-style-type: none"> ▪ Procedure should be as fast and simple as possible 	<ul style="list-style-type: none"> ▪ SA's practice
Lithuania	<ul style="list-style-type: none"> ▪ Four to six-month time-limit to investigate or inspect, but this time-limit does not apply in case of an OSS procedure 	<ul style="list-style-type: none"> ▪ National legislation: Art. 21(1) of the Law on Legal Protection of Personal Data (LGPD)

Member State/EEA State	NARs imposing deadlines impacting the moment when the draft decision has to be shared with CSAs	Origin of the rule (national legislation or SA's practice or interpretation)
	<ul style="list-style-type: none"> ▪ Four to six-month time-limit for the complaint handling procedure ▪ There are deadlines for the decision imposing administrative fines 	<ul style="list-style-type: none"> ▪ National legislation: Art. 21(2) of the LGPD ▪ National legislation: Art. 34(9) of the LGPD
Luxembourg	<ul style="list-style-type: none"> ▪ No deadlines for handling complaints but 3 months of silence implies a negative decision ▪ One month to decide to prosecute a case 	<ul style="list-style-type: none"> ▪ SA's interpretation and practice ▪ National legislation: Art. 38 of the 2018 Act and Art. 3 of the Regulation
Malta	<ul style="list-style-type: none"> ▪ No information 	<ul style="list-style-type: none"> ▪ No information
Netherlands	<ul style="list-style-type: none"> ▪ No deadlines but decisions must be reached in a reasonable period and the complainant must be informed 3 months after lodging the complaint 	<ul style="list-style-type: none"> ▪ SA's interpretation and practice
Norway	<ul style="list-style-type: none"> ▪ Decisions must be taken without undue delay 	<ul style="list-style-type: none"> ▪ SA's practice
Poland	<ul style="list-style-type: none"> ▪ Deadline of three months to deal with a complaint or to inform the complainant ▪ There are time-limits for control procedures ▪ There are time-limits for inspections 	<ul style="list-style-type: none"> ▪ National legislation and SA's interpretation: 2002 Act on Proceedings before Administrative Courts combined with 78(2) GDPR ▪ National legislation: cf. Art. 35 of the Code of Administrative Procedure (CAP) ▪ National legislation: cf. Art. 55 of the 2018 Law on Entrepreneurs
Portugal	<ul style="list-style-type: none"> ▪ Three-year time-limit for the fining procedure regarding Art. 86(5) GDPR infringements ▪ Two-year time-limit for Art. 83(4) GDPR infringements 	<ul style="list-style-type: none"> National legislation: Art. 40 of the 58/2019 Law
Romania	<ul style="list-style-type: none"> ▪ 45 to 90-day deadline to get a decision on the admissibility of the complaint ▪ The complainant should be informed within three months ▪ In case of cooperation duties, the complainant should be informed every three months ▪ Decision should be issued 45 days after the end of the investigation 	<ul style="list-style-type: none"> National legislation: Law 102/2005 and especially Art. 148 and 148(2)
Slovakia	<ul style="list-style-type: none"> ▪ 90 to 180-day deadline for the first stage decision ▪ Time-limits are suspended during investigations ▪ Time-limit of three years for the admissibility of a complaint 	<ul style="list-style-type: none"> National legislation: Art. 101(1) and (2) of the Act no. 18/2018 on Personal Data Protection (APDP)
Slovenia	<ul style="list-style-type: none"> ▪ 15 day- deadline for the first answer to a complaint ▪ Indicative two-month deadline (after receiving all the information) to handle a complaint 	<ul style="list-style-type: none"> National legislation: Art. 17 of the Decree on Administrative Operations
Spain	<ul style="list-style-type: none"> ▪ The law sets the timelines to handle complaints & investigations (nine months maximum since the decision to initiate a procedure or since the draft decision) ▪ These time limits are suspended when information must be collected or when there must be a consultation, a request for assistance or mandatory declarations, for the time between the request and the notification of the declaration to the Spanish SA 	<ul style="list-style-type: none"> National legislation: Art. 64(1), (2) and (4) of the Organic Law 3/2018 (OL 3/2018)
Sweden	<ul style="list-style-type: none"> ▪ Cases should be handled as simply, quickly and cost-efficiently as possible without risking legal certainty 	<ul style="list-style-type: none"> ▪ National legislation: Administrative Law

2.2 GENERAL TRENDS OBSERVED IN RELATION TO THE NATIONAL ADMINISTRATIVE RULES IMPOSING DEADLINES IMPACTING THE MOMENT WHEN THE DRAFT DECISION HAS TO BE SHARED WITH CSAS

In most countries, national administrative rules (national data protection laws or national general administrative laws) set **deadlines that could affect the moment on which draft decisions should be shared with other SAs**:

1. In twelve countries, national data protection laws set deadlines that could impact the moment of sharing draft decisions with other SAs:

Belgium, Cyprus, Estonia, Finland, Hungary, Italy, Lithuania, Luxembourg, Portugal, Romania, Slovakia and Spain.

2. In six countries, national general administrative laws set deadlines that could impact the moment of sharing draft decisions with other SAs:

Austria, Czech Republic, Iceland, Latvia, Poland and Slovenia.

In four countries, there are national administrative rules (national data protection laws or national general administrative laws) that provide **legal grounds to suspend or extend time-limits** in case of an OSS procedure:

1. In Austria and Hungary, national data protection laws provide for the suspension of time-limits in case of an OSS procedure.
2. In Czech Republic and Estonia, national general administrative laws provide legal grounds for extending time-limits in case of an OSS procedure.

In Italy, the time limit is suspended during an OSS procedure pursuant to Article 143.3 of the Italian Data Protection Code .

In Slovakia, time-limits are suspended during investigations (source: national data protection law) and in Spain, time limits are suspended when information must be collected or when there must be a consultation, a request for assistance or mandatory declarations, for the time between the request and the notification of the declaration to the Spanish SA.

Regarding the **moment at which draft decisions should be shared with other SAs**:

1. In seven countries, there is no exact moment when draft decisions should be shared with other SAs:
Bulgaria, Croatia, Czech Republic, Denmark, Finland Germany and Sweden.
2. In Austria, the draft decision is shared when the case is ready for decision-making (when evidence has been gathered and parties heard).
3. In six countries, the draft decision is or should be shared when the SA has adopted its decision:
Finland, France, Greece, Ireland and Italy.
4. In Belgium, the draft decision is shared when the parties have submitted their first conclusions.

2.3 QUESTIONS & CHALLENGES TO COOPERATION DUTIES STEMMING FROM THE APPLICATION OF NATIONAL ADMINISTRATIVE RULES IMPOSING DEADLINES IMPACTING THE MOMENT WHEN THE DRAFT DECISION HAS TO BE SHARED WITH CSAS

The application of national administrative rules imposing deadlines impacting the moment at which the draft decision has to be shared with CSAs may raise some questions and challenges to a smooth

implementation of the OSS mechanism.

1. It is not sure that all countries share the same definition of the term “deadlines” or at least that they have the same legal consequences (some deadlines seem to be indicative while others may relate to the admissibility of the procedure).
2. Deadlines are not the same in all the countries, which could lead to some inconsistencies when performing cooperation duties.
3. There is no coherence as to the moment when draft decisions should be shared with CSAs.
4. An issue may arise from the obligation to comply with some national administrative rules imposing strict deadlines for the pronunciation of a decision.

2.4 SUGGESTIONS AND POSSIBLE SOLUTIONS

1. Some countries provide for the suspension or the extension of time-limits or deadlines when investigating a case or when performing cooperation duties in the context of an OSS procedure. This mechanism (suspension or extension of time-limits or deadlines) could be part of a possible solution. However, the suspension or the extension of time-limits or deadlines should not be indefinite in time nor unjustified or discriminatory when comparing with other proceedings.
2. A more comprehensive solution could be the harmonisation of the applicable deadlines in the case of an OSS procedure for all countries. This harmonisation should be considered at European level (EDPB). However, due to the fact that some deadlines are fixed by national laws, guidelines may not be sufficient and a legislative initiative might therefore be required.
3. Regarding the moment when draft decisions should be shared with other CSAs, issuing guidelines at the European level (EDPB) might be the best solution.

3 NATIONAL ADMINISTRATIVE RULES REGARDING THE ADMISSIBILITY OF COMPLAINTS FROM INDIVIDUALS

3.1 OVERVIEW OF NATIONAL ADMINISTRATIVE RULES REGARDING THE ADMISSIBILITY OF COMPLAINTS FROM INDIVIDUAL

Table 2: Overview of NARs regarding the admissibility of complaints from individuals

Member State/EEA State	NARs regarding the admissibility of complaints from individuals	Origin of the rule (national legislation or SA's practice or interpretation)
Austria	<ul style="list-style-type: none"> ▪ Formal admissibility requirements ▪ Time limit to introduce the complaint 	<ul style="list-style-type: none"> ▪ National legislation: Art. 13(3) and 21.1-3 of the DSG ▪ National legislation: Art. 24(4) of the DSG
Belgium	<ul style="list-style-type: none"> ▪ Formal admissibility requirements, including language requirement for the complaint ▪ Admissibility of complaints is assessed by front office ▪ It is not clear whether complaints are admissible when they concern processing for journalistic purposes and for purposes of academic, artistic or literary expression 	National legislation: Art. 60 of the 2017 Act (cf. Art. 91 and 95 of 2017 Act for dismissal by litigation chamber and inspection service)
Bulgaria	<ul style="list-style-type: none"> ▪ Formal admissibility requirements, including language & writing requirements for the complaint 	<ul style="list-style-type: none"> ▪ National legislation: Art. 29 of the Rules on the activity of the Commission for Personal Data Protection and its administration
Croatia	<ul style="list-style-type: none"> ▪ Admissibility of complaints is ruled by the Law on Administrative Procedure 	<ul style="list-style-type: none"> ▪ National legislation: Law on Administrative Procedure
Cyprus	<ul style="list-style-type: none"> ▪ Admissibility of complaints is assessed by the Commissioner 	<ul style="list-style-type: none"> ▪ National legislation: Art. 24(d) of the Law 125(I)/2018
Czech Republic	<ul style="list-style-type: none"> ▪ No admissibility requirements 	<ul style="list-style-type: none"> ▪ No information
Denmark	<ul style="list-style-type: none"> ▪ No admissibility requirements 	<ul style="list-style-type: none"> ▪ No information
Estonia	<ul style="list-style-type: none"> ▪ No specific provision on complaints' admissibility requirements other than Administrative Procedure Act or Law Enforcement Act (normally no formal requirement as such but there might be internal thresholds at the SA level) 	<ul style="list-style-type: none"> ▪ National legislation: Administrative Procedure Act and Law Enforcement Act ▪ SA's practice (for internal thresholds)
Finland	<ul style="list-style-type: none"> ▪ Formal admissibility requirements 	<ul style="list-style-type: none"> ▪ No clear indication
France	<ul style="list-style-type: none"> ▪ Condition of prior exercise of data subject's (DS's) rights 	<ul style="list-style-type: none"> ▪ National legislation: Art. 49 of the Règlement intérieur de la CNIL (CNIL RoI)
Germany	<ul style="list-style-type: none"> ▪ No requirement for complaints' admissibility (even anonymous complaints are processed) 	<ul style="list-style-type: none"> ▪ No information
Greece	<ul style="list-style-type: none"> ▪ Manifestly vague, unfounded, improperly or anonymously lodged questions or complaints may be dismissed 	<ul style="list-style-type: none"> ▪ National legislation: Art. 13(2) of the Law 4624/2019
Hungary	<ul style="list-style-type: none"> ▪ Dismissal of minor infringements ▪ Dismissal of anonymous complaints 	<ul style="list-style-type: none"> ▪ National legislation: Art. 52 of the Act CXII of 2011 ▪ National legislation: Art. 53(2) and (3) of the Act CXII of 2011
Iceland	<ul style="list-style-type: none"> ▪ No information 	<ul style="list-style-type: none"> ▪ No information
Ireland	<ul style="list-style-type: none"> ▪ Irish SA (Data Protection Commissioner - DPC) does not have the same level of discretion in handling complaints as in some other countries; the DPC noted that this could lead to some difficulties in some cross-border cases where the DPC is not the 	<ul style="list-style-type: none"> ▪ SA's practice or interpretation

Member State/EEA State	NARs regarding the admissibility of complaints from individuals	Origin of the rule (national legislation or SA's practice or interpretation)
	<p>LSA</p> <ul style="list-style-type: none"> ▪ Admissibility requirements including language (in either Irish or English (Official Languages Act, 2003)) ▪ The SA carries out an initial examination of complaints received ▪ No implementation of Article 80(2) GDPR 	<ul style="list-style-type: none"> ▪ Section 107 of the 2018 Act ▪ Section 109 of the 2018 Act ▪ No information
Italy	<ul style="list-style-type: none"> ▪ Formal admissibility requirements 	<ul style="list-style-type: none"> ▪ National legislation: Art. 142 of the Legislative Decree No 196/2003
Latvia	<ul style="list-style-type: none"> ▪ Formal admissibility requirements ▪ Complaint can be dismissed in case of previous investigation by the Inspectorate 	<ul style="list-style-type: none"> ▪ National legislation: Art. 3 of the Law on Submission ▪ National legislation: cf. Art. 7 of the Law on Submission
Liechtenstein	<ul style="list-style-type: none"> ▪ No information 	<ul style="list-style-type: none"> ▪ No information
Lithuania	<ul style="list-style-type: none"> ▪ Obligation to investigate all complaints ▪ Condition of prior exercise of DS's rights 	<ul style="list-style-type: none"> ▪ National legislation: Art. 27(1)(1-8) of the LGPD
Luxembourg	<ul style="list-style-type: none"> ▪ Discretionary power when assessing complaints' admissibility 	<ul style="list-style-type: none"> ▪ SA's practice or interpretation
Malta	<ul style="list-style-type: none"> ▪ Complaints non admissible when no sufficient grounds to launch an investigation or no violation of DS' rights 	<ul style="list-style-type: none"> ▪ SA's practice or interpretation
Netherlands	<ul style="list-style-type: none"> ▪ Formal admissibility requirements ▪ The DS must qualify as an interested party ▪ Complaints are dismissed if they concern processing for journalistic purposes and for purposes of academic, artistic or literary expression 	<ul style="list-style-type: none"> ▪ National legislation: cf. Art. 4(1)-(5) of the General Administrative Law Act (GALA) ▪ National legislation: cf. Art. 1(2) of GALA ▪ National data protection law or SA's interpretation (?)
Norway	<ul style="list-style-type: none"> ▪ Duty to investigate all complaints regarding a possible data protection breach ▪ NSA considers that all complaints (Art. 57(1)(f) GDPR) should be handled by the SA 	<ul style="list-style-type: none"> ▪ SA's interpretation
Poland	<ul style="list-style-type: none"> ▪ Formal admissibility requirements 	<ul style="list-style-type: none"> ▪ National legislation: Art. 61(a), 63(2) and 64 of the CAP
Portugal	<ul style="list-style-type: none"> ▪ If the GDPR infringement is also a criminal offence, the Portuguese SA (CNPD) is not competent (public prosecutor will be solely competent to act) 	<ul style="list-style-type: none"> ▪ National legislation: Art. 55 of the Law 58/2019
Romania	<ul style="list-style-type: none"> ▪ Time limit of 45 to 90 days to get a decision on the admissibility of the complaint 	<ul style="list-style-type: none"> ▪ National legislation: Art. 148(2) of the Law amending and supplementing Law no. 102/2005
Slovakia	<ul style="list-style-type: none"> ▪ Complaints are inadmissible when reviewed at the same time by a court or a law enforcement authority or when DS does not cooperate ▪ Time limit of three years to introduce the complaint 	<ul style="list-style-type: none"> ▪ National legislation: Art. 100(5) of the APDP
Slovenia	<ul style="list-style-type: none"> ▪ Formal admissibility requirements applicable to complaints in the Inspection procedure ▪ Formal admissibility requirements applicable to complaints in the Administrative Procedure 	<ul style="list-style-type: none"> ▪ National legislation: Art. 24 of the Inspection Act ▪ National legislation: Art. 66(1) of the General Administrative Procedure Act
Spain	<ul style="list-style-type: none"> ▪ Formal admissibility requirements: description of the complaint is required ▪ Dismissal is possible when DC/DP has taken corrective measures or when no damage to DS or DS's rights are guaranteed by the implantation of 	<ul style="list-style-type: none"> ▪ National legislation: Arts. 64-65 of Organic Law 3/2018

Member State/EEA State	NARs regarding the admissibility of complaints from individuals	Origin of the rule (national legislation or SA's practice or interpretation)
Sweden	<p>the measures</p> <ul style="list-style-type: none"> ▪ Admissibility of complaints: the SA distinguishes between request (57(4) GDPR) and complaint (57(1)(f) GDPR). It proceeds to an individual assessment of any case on a risk-based approach as laid down in the Supervision Policy 	<ul style="list-style-type: none"> ▪ SA's practice & interpretation

3.2 GENERAL TRENDS OBSERVED IN RELATION TO THE NATIONAL ADMINISTRATIVE RULES REGARDING THE ADMISSIBILITY OF COMPLAINTS FROM INDIVIDUALS

Complaints from individuals must usually comply with requirements laid down by national administrative rules stipulated either in national data protection laws and/or in national general administrative laws (e.g. formal requirements including the identification of the complainant, prior exercise of data subject's rights, substantiation of the complaint, language requirements or deadlines). Failing to meet these requirements might lead to the (early) dismissal of the complaint - but not always.

1. The admissibility of complaints from individuals is conditional upon compliance with the formal requirements laid down in the national data protection laws in 13 countries:
Austria, Belgium, Bulgaria, France, Greece, Hungary, Ireland, Italy, Lithuania, Portugal, Romania, Slovenia (regarding the Inspection procedure) and Spain.
2. The admissibility of complaints from individuals is conditional upon compliance with the formal requirements laid down in national general administrative rules in seven countries:
Croatia, Estonia, Ireland (language requirement), Latvia, the Netherlands, Slovenia (regarding the Administrative Procedure) and Poland.
3. There are no formal requirements for the admissibility of complaints from individuals in four countries:
Czech Republic, Denmark, Germany and Norway.
4. In Luxembourg, the national supervisory authority has a discretionary power when assessing complaints from individuals.
5. Two countries explicitly impose the use of official languages for drafting the complaint:
Belgium and Bulgaria.
6. In France, the admissibility of complaints from individuals is formally conditional upon the prior exercise of data subject's rights such as the right to access.
7. In Slovakia, complaints from individuals are not admissible when they are reviewed by a court or a law enforcement authority.
8. In Portugal, the SA is not competent when the infringement constitutes a criminal offence. In this case, the Public Prosecutor will be the sole competent authority entitled to proceed.
9. Germany is the only country where anonymous complaints from individuals are admissible.
10. In Hungary, complaints might be dismissed on ground of minor importance.
11. In Malta, complaints from individuals are not admissible when there are not enough grounds to launch an investigation or no violation of data subject's rights.
12. In Spain, complaints from individuals may be dismissed when the controller or the processor has taken corrective measures or when there is no damage for the data subject or when the data subject's rights are guaranteed by the implementation of the corrective measures.

13. In Belgium and in the Netherlands, it is not clear whether complaints are admissible if they concern processing for journalistic purposes and for purposes of academic, artistic or literary expression.
14. In Austria and in Slovakia, there is a time-limit for complaints introduced by individuals.

3.3 QUESTIONS & CHALLENGES TO COOPERATION DUTIES STEMMING FROM THE APPLICATION OF NATIONAL ADMINISTRATIVE RULES REGARDING THE ADMISSIBILITY OF COMPLAINTS FROM INDIVIDUALS

The application of national administrative rules on complaints' admissibility may raise some questions and challenges to a smooth implementation of the OSS mechanism.

1. The Swedish SA stresses the distinction between complaints (Article 57(1) of the GDPR) and requests (Article 57(4) of the GDPR). The SA insists on the legal consequences to be deduced from this distinction. In its view, all complaints must be processed. Requests may only be dismissed on grounds laid down by Article 57(4) of the GDPR. It is not clear whether all Member States share this interpretation of these provisions of the GDPR.
2. In general, national legislation laid down requirements for the admissibility of complaints. But, the nature and the content of these requirements vary from one country to another (identification of the complainant, signature of the complainant, deadlines, content of the complaint, description of the facts, identification of the controller and processor, prior exercise of data subject's rights, language, time-limit, violation of data subject's rights, damage to data subject, etc.). It means that one complaint could be admissible in one country while not in another. This could lead to difficulties for the OSS procedure if the application of laws of CSA and LSA leads to different results.
3. It is not clear either whether the OSS procedure is followed when a complaint is deemed inadmissible for whatever reason. Notably, it is not clear whether there is any information shared with other CSAs.
4. There are obvious reasons why national legislation and practices set admissibility rules (e.g. to ensure the efficiency of the procedure and procedural motives). At the same time, however, such national rules and practices can hinder the identification of serious breaches in the implementation of the GDPR rules in cross-border processing. This is true in particular if there is no sharing of information about non-admissible cases between the SAs.

3.4 SUGGESTIONS AND POSSIBLE SOLUTIONS

In our view, the main issue with the non-admissibility of complaints from individuals decided on grounds of national administrative rules or practices is that there might be no sharing of information with other SAs about the possible cross-border processing involved in the complaint, which could contribute to a (relative) weakening of the level of data protection in Europe. In other words, it could lead to some missed opportunities when trying to identify data protection infringements at European level.

At this stage, the minimalistic solution could be to issue guidelines regarding the sharing of information on complaints from individuals related to cross-border processing, which have been deemed non-admissible by SAs.

It might be advisable to first gather best practices from SAs on the admissibility of complaints from individuals, and then to try and issue guidelines at the level of the EDPB, which would help to harmonise the criteria for addressing complaints from individuals (the intention could be to opt for the maximum information to be sure to meet all MS requirements but without creating unjustified obstacles to the data subject's right to complain). These guidelines should cover aspects which have been identified when analysing the national administrative rules on the admissibility of complaints from individuals and

include the following information in particular:

1. paper procedure or/and electronic procedure,
2. identification of the complainant,
3. signature of the complainant,
4. time-limit for introducing a complaint,
5. content of the complaint,
6. description of the facts,
7. identification of controller and processor,
8. prior exercise of data subject's rights,
9. violation of data subject's rights,
10. deadlines for addressing the complaint,
11. language to be used by complainant,
12. damage suffered by data subject, etc.

4 NATIONAL ADMINISTRATIVE RULES ON THE RIGHT TO BE HEARD

4.1 OVERVIEW OF NATIONAL ADMINISTRATIVE RULES ON THE RIGHT TO BE HEARD

Table 3: Overview of NARs on the right to be heard

Member State/EEA State	NARs on the right to be heard	Origin of the rule (national legislation or SA's practice or interpretation)
Austria	<ul style="list-style-type: none"> ▪ Parties must be heard on any piece of evidence and this has to be done before consulting CSAs 	▪ SA's practice
Belgium	<ul style="list-style-type: none"> ▪ Hearing may take place when the case is ready ▪ There is no indication if this should occur before/after consulting CSAs 	National legislation: Art. 98 of the 2017 Act
Bulgaria	<ul style="list-style-type: none"> ▪ Hearing of the parties at the meeting of the SA ▪ CSAs should be consulted before the hearing or at least in parallel with the hearing 	SA's practice
Croatia	<ul style="list-style-type: none"> ▪ There is no indication of a duty to hear the parties but they can submit statements anytime during the proceedings 	<ul style="list-style-type: none"> ▪ National legislation: cf. Art. 30 of the Law on Administrative Procedure
Cyprus	<ul style="list-style-type: none"> ▪ Hearing possible before the submission of the draft decision to CSAs 	▪ SA's practice
Czech Republic	<ul style="list-style-type: none"> ▪ No information 	▪ No information
Denmark	<ul style="list-style-type: none"> ▪ There is no specific provision in the national data protection law regarding the hearing of the parties 	▪ No information
Estonia	<ul style="list-style-type: none"> ▪ There should be a hearing of the parties 	<ul style="list-style-type: none"> ▪ National legislation: Art. 40 of the Administrative Procedure Act
Finland	<ul style="list-style-type: none"> ▪ Parties should be heard before a decision is made ▪ The hearing should happen after sharing the draft decision (for DS's complaint) ▪ Regarding fining procedure, CSAs are informed of the hearing 	<ul style="list-style-type: none"> ▪ National Administrative Legislation ▪ SA's practice ▪ SA's practice
France	<ul style="list-style-type: none"> ▪ There seems to be no duty to hear DC and/or DP before the Chair but well before the Restricted Committee ▪ There will be a second round of hearing before the Restricted Committee in case of relevant and reasoned objections from CSAs 	SA's practice
Germany	<ul style="list-style-type: none"> ▪ Parties must be heard before the issuing of the administrative act 	▪ No information
Greece	<ul style="list-style-type: none"> ▪ Parties must be heard before the draft decision 	▪ SA's practice
Hungary	<ul style="list-style-type: none"> ▪ In the course of the procedure, the party may make a statement or observation at any time 	<ul style="list-style-type: none"> ▪ Section 5 of Act CL of 2016 on the Code of General Administrative Procedure
Iceland	<ul style="list-style-type: none"> ▪ Parties should be heard before a decision is made 	<ul style="list-style-type: none"> ▪ National legislation: Art. 13 of APA
Ireland	<ul style="list-style-type: none"> ▪ It is always necessary to contact the DC/DP and let them be heard: the respondent is entitled to be heard in relation to the case against it (the respondent must be heard before the draft decision is circulated via the Article 60 process because, if no objections are raised, the SA will be required by Article 60(7) of the GDPR to adopt the decision. If, in such a case, the respondent has not been afforded their right to be heard prior to circulation of the draft decision, the respondent will have been deprived of their right to be heard) 	<ul style="list-style-type: none"> ▪ SA's practice and interpretation of the law
Italy	<ul style="list-style-type: none"> ▪ Parties have the right to be heard throughout the 	▪ Article 166(6) of the Italian

Member State/EEA State	NARs on the right to be heard	Origin of the rule (national legislation or SA's practice or interpretation)
	investigational steps and before the adoption of any corrective measures or administrative fines (except for urgent situations) ▪ There is no indication on when to consult CSAs but in practice CSAs are kept in the loop at all stages of the proceeding	Data Protection Code
Latvia	▪ Parties must be heard before the draft decision	▪ National legislation: cf. APL
Liechtenstein	▪ Parties should have a reasonable opportunity to present their case before the consultation of CSAs	▪ SA's practice
Lithuania	▪ Parties are heard before the draft decision is sent to CSAs	▪ SA's practice
Luxembourg	▪ Parties have the right to be heard during all the phases leading to a final decision. This should take place before consulting CSAs	▪ SA's practice
Malta	▪ Parties are heard or asked to make submissions at the investigation stage. There is no right to be heard before the decision is issued	▪ SA's practice
Netherlands	▪ Parties may present their views on the investigating report in case of an OSS procedure so that it can be taken into account in the draft decision	▪ SA's practice
Norway	▪ Duty to hear the parties during the fact-finding phase and during the phase of notification of the intent to make a decision	▪ SA's practice
Poland	▪ Parties are heard before the consultation with CSAs and before the draft decision is submitted to them ▪ For cross-border cases the draft decision is submitted to other SAs after notification to the complainant and to DC/DP to allow them to express their views on the evidence and materials collected and claims made	National legislation: cf. Art. 10(1) of the CAP
Portugal	▪ Hearing of the DC/DP after sharing the draft decision	▪ SA's practice
Romania	▪ No information	▪ No information
Slovakia	▪ Parties have the right to be heard in the official administrative proceedings	▪ SA's practice
Slovenia	▪ Parties have the right to be heard before decision-making and before consulting CSAs	▪ National legislation: cf. Art. 29 of the Inspection Act and Art. 9(1) of the General Administrative Procedure Act
Spain	▪ Parties must be heard when the case is ready and before the definite draft decision ▪ There is no indication on the consultation with CSAs	▪ SA's practice ▪ No information
Sweden	▪ Discretionary power to hear the parties	▪ SA's practice

4.2 GENERAL TRENDS OBSERVED IN RELATION TO THE NATIONAL ADMINISTRATIVE RULES ON THE RIGHT TO BE HEARD

Deriving from the **SA's practices** it seems that in most countries, the parties involved in an OSS procedure have the right to be heard. The extent to which these rules are based on national general administrative laws (national data protection laws or national general administrative rules) is not always clear. This is due to the fact that the sources consulted did not systematically specify the legal basis of the rules. With this caveat in mind, the following trends could be identified:

1. In seventeen countries, the right to be heard is based upon the practice of the SAs:
Austria, Bulgaria, Cyprus, Finland, France, Greece, Ireland, Liechtenstein, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Portugal, Slovakia, Spain and Sweden.
2. In six countries, the right to be heard (in a broad sense) is based upon national general

administrative laws:

Croatia, Estonia, Iceland, Latvia, Poland and Slovenia,

3. In Belgium and Italy, the national data protection law recognises the right to be heard.

It is not clear whether **data subjects** have the right to be heard or whether this right benefits only the **controllers or processors**.

Regarding the **moment when parties should be heard**:

1. In Malta and Norway, parties are heard during the investigation stage or the fact-finding phase.
2. In Germany, Iceland and Slovenia, parties should be heard before making a decision.
3. In five countries, parties must be heard before the draft decision:
4. Greece, Latvia, The Netherlands, Poland and Spain.
5. In seven countries, parties should be heard before consulting other SAs:
6. Austria, Bulgaria, Cyprus, Liechtenstein, Lithuania, Poland and Slovenia.
7. In Finland and Portugal, parties should be heard after sharing the draft decision.
8. In Belgium, there is no indication whether the hearing of the parties should occur before or after consulting other SAs.
9. In France, there will be a second round of hearing in case of relevant and reasoned objections from CSAs.
10. In Ireland, the respondent must be heard before the draft decision is circulated.

4.3 QUESTIONS & CHALLENGES TO COOPERATION DUTIES STEMMING FROM THE APPLICATION OF NATIONAL ADMINISTRATIVE RULES ON THE RIGHT TO BE HEARD

The right to be heard exists to some extent in 25 countries. However, there is no harmonisation as to who should be heard (the ones under investigation or the complainants or the data subjects) nor as to the moment when parties should be heard: during the investigation or the fact-finding phase, before or after sharing the draft decision.

The non-respect of the right to be heard at national level could jeopardise the validity of decisions adopted in an OSS procedure e.g. on the ground of violation of a fundamental right of the prosecuted party.

4.4 SUGGESTIONS AND POSSIBLE SOLUTIONS

1. It is recommended for the EDPB to issue a declaration (or similar) highlighting the importance of, or even the fundamental nature of, the right to be heard in the context of OSS proceedings.
2. At the same time, we should consider the procedural position of the parties to be heard. Indeed, the fact that parties must be heard does not per se imply that they are parties at the procedure (from a procedural point of view). They may be only concerned by the procedure or be the ones under investigation without formally being parties in the procedure. In other words, we should assess the determination of the parties who are procedurally involved in the OSS procedure and of those who are only concerned by the procedure. Article 41 of the EU Charter offers every person (physical or legal) the right to be heard before any individual measure that would adversely affect him or her is taken.
3. We should then consider the practical aspects of the right to be heard: should it be exercised written or orally, or both and at what time and in the presence of what parties (SA, CSA, data subjects, etc.)? At EU level, case law exists on this and it is possible for it to be exercised in

written form only.

5 NATIONAL ADMINISTRATIVE RULES ON AMICABLE SETTLEMENTS

5.1 OVERVIEW OF NATIONAL ADMINISTRATIVE RULES ON AMICABLE SETTLEMENTS

Table 4: Overview of NARs regarding rules on amicable settlements

Member State/EEA State	NARs on amicable settlements	Origin of the rule (national legislation or SA's practice or interpretation)
Austria	▪ Amicable settlements are possible between DC/DP & complainant	▪ National legislation: Art. 24(6) of DSG
Belgium	▪ Amicable settlements are possible between DC/DP & complainant	▪ SA's practice or interpretation
Bulgaria	▪ Amicable settlements are possible	▪ National legislation: Art. 20 of the APC
Croatia	▪ Amicable settlements are not provided for under the national GDPR Law (LoLoGDPR)	▪ No information
Cyprus	▪ The notion of amicable settlement does not exist in national law, but it could be used in data protection	▪ SA's interpretation
Czech Republic	▪ Czech law knows the notion of amicable settlement but it is not applied by the SA in this sense: in practice, the SA may discontinue a case when the purpose of the proceedings has been achieved	▪ SA's interpretation and practice based on Art. 65 of the Act No 110/2019
Denmark	▪ Amicable settlements are not possible between DC/DP and SA	▪ SA's interpretation
Estonia	▪ Amicable settlement does not exist in data protection legislation, but it could be implemented thanks to the Administrative Procedure Act	▪ SA's interpretation based on Art. 95 of the Administrative Procedure Act
Finland	▪ Amicable settlements are possible between DC/DP and complainant	▪ SA's interpretation
France	▪ No information	▪ No information
Germany	▪ Amicable settlements are possible between DC/DP and complainant but not between SA and DC/DP	▪ No information
Greece	▪ It is not possible for the SA to conclude an amicable settlement	▪ SA's interpretation
Hungary	▪ Amicable settlements between DC/DP and complainant are possible	▪ National legislation: cf. Arts. 51(A)-58 of the 2011 Act CXII and by the Section 75 and 83 of Act CL of 2016 of the Code of General Administrative Procedure (CGAP)
Iceland	▪ Amicable settlements between DC/DP and complainant are possible	▪ SA's interpretation
Ireland	▪ Amicable settlements between DC/DP and complainant are possible ▪ When reaching an amicable settlement, the complaint is deemed to have been withdrawn (but the SA may pursue its own inquiry, if it deems fit)	▪ National legislation: Art. 109 of the DPA ▪ SA's practice
Italy	▪ Amicable settlements between DC/DP and complainant are possible	▪ SA's interpretation based on Art. 57(1) and 77(1) of the GDPR
Latvia	▪ Amicable settlements are possible and it seems to be possible between the SA and DC/DP	▪ SA's interpretation based on Art. 80(1) of the APL
Liechtenstein	▪ Amicable settlements are possible	▪ No information
Lithuania	▪ National Law on legal protection of personal data does not regulate amicable settlements	▪ No information
Luxembourg	▪ The Luxembourg SA (CNPD) always seeks to find a	▪ SA's practice

Member State/EEA State	NARs on amicable settlements	Origin of the rule (national legislation or SA's practice or interpretation)
	conciliating solution	
Malta	▪ Amicable settlements are envisaged	▪ No information
Netherlands	▪ The Dutch SA may mediate the parties	▪ SA's interpretation and practice
Norway	▪ There is no formal concept of amicable settlement in Norwegian law. But it is possible to solve the case in ways other than with a sanction	▪ SA's interpretation
Poland	▪ Amicable settlements between the SA and DC/DP are not possible ▪ Amicable settlements only possible for cross-border cases with local impacts only	SA's interpretation based on Recital 131 and Art. 56(2) of the GDPR
Portugal	▪ Amicable settlements are not possible	▪ No information
Romania	▪ No information	▪ No information
Slovakia	▪ Amicable settlements are possible between DC/DP and complainant	▪ No information
Slovenia	▪ Formally, there are no amicable settlements possible	▪ No information
Spain	▪ Amicable settlements are possible between DC/DP and complainant	▪ National legislation: Art. 37(2) and 65(3) of the OL 3/2018
Sweden	▪ Amicable settlements are not possible	▪ No information

5.2 GENERAL TRENDS OBSERVED IN RELATION TO THE NATIONAL ADMINISTRATIVE RULES ON AMICABLE SETTLEMENTS

Amicable settlements between controllers or processors and data subjects as complainants are possible in most countries whether on grounds of national data protection laws or of national general administrative laws. We received no clear information or indication on whether the conclusion of amicable settlements would take place prior to the consultation of CSAs on draft decisions.

1. In three countries, amicable settlements between controllers or processors and complainants are possible on grounds of national data protection laws:
2. Austria, Hungary and Ireland.
3. In three countries, amicable settlements between controllers or processors and complainants are possible on grounds of national general administrative laws.
4. Bulgaria, Estonia and Latvia.
5. In twelve countries, amicable settlements between controllers or processors and complainants are deemed possible, but with no clear view or indication on the legal basis:
6. Belgium, Finland, Germany, Hungary, Iceland, Italy, Liechtenstein, Luxembourg, Malta, the Netherlands, Slovakia and Spain.
7. In three countries, amicable settlements between controllers or processors and complainants are not possible:
8. Portugal, Slovenia and Sweden.
9. In Cyprus and Norway, amicable settlements between controllers or processors and complainants do not exist on grounds of national general administrative laws, with no indication on their possibility on other legal grounds.
10. In six countries, we received a clear indication that amicable settlements between controllers or processors and SAs are not possible:
11. Denmark, Germany, Poland, Portugal, Slovenia and Sweden.

12. In Latvia, amicable settlements between controllers or processors and SAs are possible on ground of SA's interpretation or practice.
13. In Poland, amicable settlements are possible for cross-border cases with local impact only.

5.3 QUESTIONS & CHALLENGES TO COOPERATION DUTIES STEMMING FROM THE APPLICATION OF NATIONAL ADMINISTRATIVE RULES ON AMICABLE SETTLEMENTS

The application of national administrative rules on amicable settlements may raise some questions and challenges to a smooth implementation of the OSS mechanism.

1. The possibility to reach an amicable settlement between controllers or processors and complainants does not exist in all countries. This might become problematic in cases where countries acknowledging amicable settlements and countries that do not acknowledge such settlements engage in an OSS procedure.
2. Amicable settlements between the SA and controllers or processors are explicitly possible in Latvia. But this kind of settlement is not possible in at least six other countries (it cannot be said whether it is possible or impossible in the other countries). Again, this might become problematic in cases where countries that acknowledge amicable settlements engage in an OSS procedure with countries that do not acknowledge such settlements.
3. There might be a controversy on whether amicable settlements are possible for cross-border cases with a broader impact than just locally.
4. Where amicable settlements are reached, there is no clear indication on their impact on the OSS procedure - in particular on whether and when this information will be shared with the other relevant SAs. This in turn means that even if parties enter in an amicable settlement in one country, this fact does not preclude initiation or continuation of the procedure in any other country in case of cross-border procedures.

5.4 SUGGESTIONS AND POSSIBLE SOLUTIONS

The best solution is to draft comprehensive Guidelines on amicable settlements in an OSS procedure at the European (EDPB) level with a specific focus on the sharing of information on amicable settlements between SAs (eventually before their finalisation stage) and their legal effects for the parties concerned (including the data subjects).

6 NATIONAL ADMINISTRATIVE RULES ON THE PRIOR NOTIFICATION OF FORTHCOMING INVESTIGATIONS OR EXERCISE OF CORRECTIVE POWERS

6.1 OVERVIEW OF NATIONAL ADMINISTRATIVE RULES ON THE PRIOR NOTIFICATION OF FORTHCOMING INVESTIGATIONS OR EXERCISE OF CORRECTIVE POWERS

Table 5: Overview of NATs on the prior notification of forthcoming investigations or exercise of corrective powers

Member State/EEA State	NARs on the prior notification of forthcoming investigations or exercise of corrective powers	Origin of the rule (national legislation or SA's practice or interpretation)
Austria	<ul style="list-style-type: none"> ▪ No obligation to notify DC/DP of forthcoming investigation or exercise of corrective powers 	<ul style="list-style-type: none"> ▪ SA's interpretation
Belgium	<ul style="list-style-type: none"> ▪ No obligation to notify DC/DP of forthcoming investigation or exercise of corrective powers 	<ul style="list-style-type: none"> ▪ SA's interpretation
Bulgaria	<ul style="list-style-type: none"> ▪ DC/DP are immediately notified of forthcoming investigation or exercise of corrective powers 	<ul style="list-style-type: none"> ▪ SA's practice
Croatia	<ul style="list-style-type: none"> ▪ Obligation to notify DC/DP of forthcoming investigation or exercise of corrective powers (e.g. obligation to notify the DC/DP/DS of joint investigations (including the presence of representatives of other SA's) before the operation) ▪ But there might be unannounced and announced supervisions onsite 	<ul style="list-style-type: none"> ▪ National legislation: cf. Art. 15(4) of the LoIoGDPR ▪ SA's practice
Cyprus	<ul style="list-style-type: none"> ▪ <u>Forthcoming investigation:</u> no obligation to notify DC/DP ▪ <u>Forthcoming exercise of corrective powers:</u> DC/DP have the right to be heard before drafting a decision; the latter will then be submitted to CSAs 	<ul style="list-style-type: none"> ▪ SA's practice and interpretation
Czech Republic	<ul style="list-style-type: none"> ▪ Obligation to notify DC/DP of a forthcoming investigation or exercise of corrective powers: the parties to proceedings have to be notified about the initiation of the proceedings 	<ul style="list-style-type: none"> ▪ SA's practice and interpretation
Denmark	<ul style="list-style-type: none"> ▪ Obligation to notify DC/DP of forthcoming investigation or exercise of corrective powers ▪ There will be some contact between DC/DP with the SA if the decision is not going to be favourable and the party must know that the Danish SA has some specific information in order to allow the party to make a statement 	<ul style="list-style-type: none"> ▪ SA's practice and interpretation based on national administrative rules
Estonia	<ul style="list-style-type: none"> ▪ No information 	<ul style="list-style-type: none"> ▪ No information
Finland	<ul style="list-style-type: none"> ▪ No obligation to notify DC/DP of a forthcoming investigation or exercise of corrective powers except for onsite inspection ▪ But notification of the starting time of the inspection except if this would jeopardise it 	<ul style="list-style-type: none"> ▪ SA's practice and interpretation ▪ National legislation: cf. Art. 39 of the Administrative Procedure Act
France	<ul style="list-style-type: none"> ▪ <u>Forthcoming investigation:</u> no prior information ▪ <u>Forthcoming exercise of corrective powers:</u> no prior notification of Chair's Decision but for Decisions issued by the Restricted Committee, DC/DP are informed of the designation of a Rapporteur (the draft report is notified to DC/DP, the latter will be heard during the restricted session and they may produce observations – the decision is notified to the controller) 	<ul style="list-style-type: none"> ▪ National legislation: Art. 26 of the Decree ▪ National legislation: Art. 20-23 of the LIL Act and Art. 38-45 of the Decree
Germany	<ul style="list-style-type: none"> ▪ Obligation to notify DC/DP of forthcoming investigation or exercise of corrective powers: participants of a case have the right to be heard and inspect documents 	<ul style="list-style-type: none"> ▪ National legislation: cf. Arts. 28-29 of the Federal Administrative Procedures Act (VwVfG)
Greece	<ul style="list-style-type: none"> ▪ No obligation to notify DC/DP of forthcoming investigation or exercise of corrective powers 	<ul style="list-style-type: none"> ▪ No information

Member State/EEA State	NARs on the prior notification of forthcoming investigations or exercise of corrective powers	Origin of the rule (national legislation or SA's practice or interpretation)
Hungary	<ul style="list-style-type: none"> ▪ No obligation to contact DC/DP for a mere inquiry ▪ But in case of an Authority procedure for data protection, DC/DP must be notified at the beginning of the procedure (there are exceptions) 	<ul style="list-style-type: none"> ▪ Section 104 (3) of Act CL of 2016
Iceland	<ul style="list-style-type: none"> ▪ Obligation to notify DC/DP of forthcoming investigation or exercise of corrective powers 	<ul style="list-style-type: none"> ▪ National legislation: cf. Arts. 13-14 of the APA
Ireland	<ul style="list-style-type: none"> ▪ Obligation to notify DC/DP of forthcoming investigation or exercise of corrective powers: DC should be contacted or notified during the investigation of a complaint: <ol style="list-style-type: none"> 1. The respondent is entitled to notice of the complaint made against them; 2. The respondent is entitled to know the details of the case against them; 3. The respondent is entitled to be heard in relation to the case against them (the respondent must be heard before the draft decision is circulated via the Article 60 process because, if no objections are raised, the SA will be required by Article 60(7) of the GDPR to adopt the decision. If, in such a case, the respondent has not been afforded the right to be heard prior to circulation of the draft decision, the respondent will have been deprived of their right to be heard) 	<ul style="list-style-type: none"> ▪ SA's practice
Italy	<ul style="list-style-type: none"> ▪ Obligation to notify DC/DP of forthcoming investigation or exercise of corrective powers before adopting corrective powers or imposing administrative fines ▪ DC/DP should be notified before starting an OSS procedure 	<ul style="list-style-type: none"> ▪ National legislation: Art. 166 of the IDPC ▪ SA's interpretation
Latvia	<ul style="list-style-type: none"> ▪ Obligation to notify DC/DP of forthcoming investigation 	<ul style="list-style-type: none"> ▪ National legislation: Art. 15 of the PDP Law
Liechtenstein	<ul style="list-style-type: none"> ▪ Notification before accessing the premises of DC/DP and before consulting SAs 	<ul style="list-style-type: none"> ▪ National legislation: Art. 17 of the Data Protection Act (DPA)
Lithuania	<ul style="list-style-type: none"> ▪ No obligation to notify DC/DP of forthcoming investigation or exercise of corrective powers before a final decision is made. The draft decision is only submitted to CSAs but not to DC/DP (they only receive the final decision) 	<ul style="list-style-type: none"> ▪ SA's interpretation and practice
Luxembourg	<ul style="list-style-type: none"> ▪ Forthcoming investigation: notification of the opening of an investigation (except when unexpected visit is necessary) before consulting other CSAs ▪ Forthcoming exercise of corrective powers: notification of the DC/DP before consulting other CSAs 	<ul style="list-style-type: none"> ▪ National legislation: Art. 8(1) of the Regulation ▪ SA's practice
Malta	<ul style="list-style-type: none"> ▪ Not always an obligation to notify DC/DP of a forthcoming investigation or exercise of corrective powers 	<ul style="list-style-type: none"> ▪ SA's interpretation
Netherlands	<ul style="list-style-type: none"> ▪ Obligation to notify DC/DP of forthcoming investigation or exercise of corrective powers to some extent 	<ul style="list-style-type: none"> ▪ SA's interpretation
Norway	<ul style="list-style-type: none"> ▪ Obligation to notify DC/DP before making an administrative decision (no precision if this should occur before/after consulting CSA on the draft decision) 	<ul style="list-style-type: none"> ▪ National legislation: Art. 16 of the Personal Data Act (PAA)
Poland	<ul style="list-style-type: none"> ▪ Obligation to notify DC/DP of forthcoming investigation or exercise of corrective powers: in practice, 7 days' notice before the inspection 	<ul style="list-style-type: none"> ▪ National legislation: cf. Art. 48 of the 2018 Law on Entrepreneurs
Portugal	<ul style="list-style-type: none"> ▪ No obligation to notify DC/DP of forthcoming investigation or exercise of corrective powers 	<ul style="list-style-type: none"> ▪ SA's interpretation
Romania	<ul style="list-style-type: none"> ▪ No information 	<ul style="list-style-type: none"> ▪ No information
Slovakia	<ul style="list-style-type: none"> ▪ The obligation to notify DC/DP of forthcoming investigation or exercise of corrective powers takes place before consulting other SAs on the draft decision 	<ul style="list-style-type: none"> ▪ National legislation: Arts. 18(3) and 33(2) of the Administrative

Member State/EEA State	NARs on the prior notification of forthcoming investigations or exercise of corrective powers	Origin of the rule (national legislation or SA's practice or interpretation)
Slovenia	<ul style="list-style-type: none"> ▪ No formal obligation to notify DC/DP of forthcoming investigation or exercise of corrective powers but it can be done 	<ul style="list-style-type: none"> ▪ Proceedings Act (APA) ▪ National legislation: cf. Art. 24(4) of the Inspection Act ▪ SA's interpretation
Spain	<ul style="list-style-type: none"> ▪ No obligation to notify DC/DP of forthcoming investigation or exercise of corrective powers ▪ But in practice, DC/DP are informed of the facts e.g. to open the way to an amicable settlement and to answer SAs' questions 	SA's practice
Sweden	<ul style="list-style-type: none"> ▪ No obligation to notify DC/DP of forthcoming investigation or exercise of corrective powers ▪ But there would be a contact with DC/DP in case of an audit 	SA's interpretation and practice

6.2 GENERAL TRENDS OBSERVED IN RELATION TO THE NATIONAL ADMINISTRATIVE RULES ON THE PRIOR NOTIFICATION OF FORTHCOMING INVESTIGATIONS OR EXERCISE OF CORRECTIVE POWERS

National administrative rules regarding the prior notification of forthcoming investigations or exercise of corrective powers show the following differences:

1. In nine countries, there is no obligation to notify controllers or processors of forthcoming investigations or exercise of corrective powers:
2. Austria, Belgium, Finland, Greece, Lithuania, Portugal, Slovenia, Spain and Sweden.
3. In Cyprus and France, there is no obligation to notify controllers or processors of forthcoming investigations.
4. In five countries, there is an obligation to notify controllers or processors of forthcoming investigations or exercise of corrective powers, based on national data protection laws:
5. Croatia, Italy, Latvia, Liechtenstein and Luxembourg (before consulting CSAs).
6. In seven countries, there is an obligation to notify controllers or processors of forthcoming investigations or exercise of corrective powers, based on national general administrative laws:
7. Denmark, Germany, Hungary (for formal request but not for a mere inquiry), Iceland, Norway, Poland and Slovakia (before consulting CSAs on the draft decision)
8. In five countries, there is an obligation to notify controllers or processors of forthcoming investigations or exercise of corrective powers, based on SA's practice:
9. Bulgaria, Czech Republic, Finland (for on-site inspection), Ireland and the Netherlands.
10. In Cyprus, there is an obligation to notify controllers or processors of a forthcoming exercise of corrective powers, based on SA's practice.
11. In France, there is an obligation to notify controllers or processors of a forthcoming exercise of corrective powers, based on national data protection laws.
12. In Malta, there is not always an obligation to notify controllers or processors of forthcoming investigations or exercise of corrective powers.
13. In Spain, controllers or processors are informed of the facts in order to open the way to amicable settlements and to allow them to answer the SA's questions.
14. In Sweden, there will be a contact with controllers or processors in case of an audit.

6.3 QUESTIONS & CHALLENGES TO COOPERATION DUTIES STEMMING FROM THE APPLICATION OF NATIONAL ADMINISTRATIVE RULES ON THE PRIOR NOTIFICATION OF FORTHCOMING INVESTIGATIONS OR EXERCISE OF CORRECTIVE POWERS

The application of national administrative rules on the prior notification of forthcoming investigations or exercise of corrective powers may raise some questions and challenges to the smooth implementation of the OSS mechanism.

1. There is no convergence between the considered countries regarding the prior notification of forthcoming investigations or exercise of corrective powers. It is an obligation in some and not in others. This could lead to the invalidation of the procedure for breaching fundamental rights of the parties involved in the procedure. It also questions the nature of the procedure and the legal effects to be attached to this notification. It also questions the procedural qualification of the parties (are they parties to the procedure or are they only concerned by the procedure?).
2. If the controllers or processors are informed before the CSAs about this, it can also affect the good cooperation between SAs.
3. The challenge would be to reach an agreement on this kind of sensitive issue and on its practical aspects.

6.4 SUGGESTIONS AND POSSIBLE SOLUTIONS

The best option would be to assess the possibility of drafting Recommendations or Guidelines at European (EDPB) level, considering the limitations in national law, specifically regarding the prior notification of investigations or exercise of corrective powers in the context of an OSS procedure and the possibility to also inform the CSAs in advance about it.

7 NATIONAL ADMINISTRATIVE RULES IMPOSING STEPS OR DECISIONS PERTAINING TO THE OSS PROCEDURE

7.1 OVERVIEW OF NATIONAL ADMINISTRATIVE RULES IMPOSING STEPS OR DECISIONS PERTAINING TO THE OSS PROCEDURE

Table 6: Overview of NARs imposing steps or decisions pertaining to the OSS procedure

Member State/EEA State	NARs imposing steps or decisions pertaining to the OSS procedure	Origin of the rule (national legislation or SA's practice or interpretation)
Austria	<ul style="list-style-type: none"> ▪ No national provision on the procedure leading to an OSS decision except the right to be heard 	<ul style="list-style-type: none"> ▪ SA's practice
Belgium	<ul style="list-style-type: none"> ▪ Procedure leading to an OSS decision: <ol style="list-style-type: none"> 1. admissibility of the complaint by the front office 2. notification of this decision to the complainant 3. forward of this decision to the litigation chamber 4. referral of the complaint to the inspection service 5. investigation by the inspection service 6. conclusion of the investigation 7. referral to the litigation chamber 8. hearing of the parties 9. second hearing of the parties 10. revised draft decision 	<ul style="list-style-type: none"> ▪ SA's practice
Bulgaria	<ul style="list-style-type: none"> ▪ Procedure leading to an OSS decision: <ol style="list-style-type: none"> 1. opinion of the Legal Proceedings and Supervision Directorate 2. decision on the admissibility of the complaint 3. arrangements with other SAs 4. examination of the merits of the complaint at an open meeting 5. adoption of a decision (information of the complainant) 	<ul style="list-style-type: none"> ▪ National legislation: Art. 35-45 of the Personal Data Protection Act (PDPA)
Croatia	<ul style="list-style-type: none"> ▪ No information 	<ul style="list-style-type: none"> ▪ No information
Cyprus	<ul style="list-style-type: none"> ▪ Procedure leading to an OSS decision: <ol style="list-style-type: none"> 1. assessment of the complaint 2. preliminary investigation 3. notification of the DC/DP 4. examination of DC/DP response 5. DC/DP informed about a breach & corrective measures & right to be heard 6. draft decision submitted to CSA 7. final decision delivered to DC/DP 8. information of DS 	<ul style="list-style-type: none"> ▪ SA's practice
Czech Republic	<ul style="list-style-type: none"> ▪ Procedure leading to an OSS decision: <ol style="list-style-type: none"> 1. data breach notification/complaint/mass media report/... 2. preliminary assessment (inspection) 3. administrative proceeding at 1st stage ▪ appeal – administrative proceeding at second stage 	<ul style="list-style-type: none"> ▪ SA's practice
Denmark	<ul style="list-style-type: none"> ▪ No information 	<ul style="list-style-type: none"> ▪ No information
Estonia	<ul style="list-style-type: none"> ▪ No information 	<ul style="list-style-type: none"> ▪ SA's interpretation of the GDPR detailed schemes, the Administrative Procedure Act, the Law Enforcement Act and the Code of Misdemeanour

Member State/EEA State	NARs imposing steps or decisions pertaining to the OSS procedure	Origin of the rule (national legislation or SA's practice or interpretation)
		Procedure
Finland	▪ Procedure leading to an OSS decision described by law	<ul style="list-style-type: none"> ▪ National legislation: Arts. 19-48 of the DPA
France	<ul style="list-style-type: none"> ▪ Procedure leading to an OSS decision: <ol style="list-style-type: none"> 1. assessment of the claim / control / data breach 2. assessment of a cross-border transfer 3. case sent through IMI 4. determination of LSA / CSA / exclusive jurisdiction 5. if LSA/CSA, investigations, no deadlines for investigations but information of the victim and sharing of all information with CSA's before submitting a draft decision 6. when CSA, CNIL waits for the draft decision; when LSA, decision taken at the end of the investigation 7. for data breach, report sent to controller/processor (1 month to answer-15 days for rapporteur, etc.) 8. end of instruction and hearing with one-month notice 9. oral hearing and CSA's may participate 10. then decision by Restricted Committee 11. for warning, reprimand, orders, etc.), written procedure then decision by the Chair 12. the draft decisions are sent via IMI 13. the final decision is notified to the data controller/processor. Complainant is informed of the outcome 14. when CSA, Restricted Committee / Chair reviews the draft decision and transmission to LSA through standard IMI process. Once the FD is adopted by the LSA and sent to the controller or processor, the CNIL informs the complainant if the complaint was lodged at the CNIL 	<ul style="list-style-type: none"> ▪ SA's practice
Germany	<ul style="list-style-type: none"> ▪ Procedure leading to an OSS decision: <ol style="list-style-type: none"> 1. determination of the competent German SA 2. investigation 3. collecting evidence 4. hearing 5. authority acts at its discretion 	<ul style="list-style-type: none"> ▪ National legislation: <ol style="list-style-type: none"> 1. Art. 19 of the BDSG 2. Art. 24 of the VwVfG 3. Art. 26 of the VwVfG 4. Art. 28 of the VwVfG 5. Art. 40 of the VwVfG
Greece	<ul style="list-style-type: none"> ▪ Procedure leading to an OSS decision: <ol style="list-style-type: none"> 1. investigation 2. hearing 3. formal initial decision (a draft decision) 4. sharing of the draft decision with CSAs 5. final decision 	<ul style="list-style-type: none"> ▪ SA's practice
Hungary	<ul style="list-style-type: none"> ▪ The procedure leading to an OSS decision is the same as for national cases 	<ul style="list-style-type: none"> ▪ National legislation: Arts. 51/A-58 and Arts. of Act CXII
Iceland	<ul style="list-style-type: none"> ▪ No information 	<ul style="list-style-type: none"> ▪ No information
Ireland	<ul style="list-style-type: none"> ▪ Procedure leading to an OSS decision: <ol style="list-style-type: none"> 1. notice of commencement issued to the respondent who will be allocated a deadline for response 2. investigation 3. preparation of a draft investigation report 4. draft report is sent to the respondent who will be allocated a deadline for response 5. completion of the report 6. submission of the finalised report to the decision-maker (with a copy to the respondent) 	<ul style="list-style-type: none"> ▪ SA's practice

Member State/EEA State	NARs imposing steps or decisions pertaining to the OSS procedure	Origin of the rule (national legislation or SA's practice or interpretation)
	<p>7. the decision-maker will inform the respondent of the commencement of the decision-making process and the procedures that will be applied</p> <p>8. separately, the decision-maker will assess the status of the respondent concerned, by reference to the concept of undertaking (as understood in the context of Article 101 TFEU)</p> <p>9. the decision-maker will then write to the respondent to explain the concept of undertaking and the impact that it will have in proceedings in the event that he/she determines that an infringement has occurred and that an administrative fine should be imposed. The letter will include the relevant facts giving rise to any presumption of decisive influence and explain how the respondent can rebut that presumption. The letter will invite the respondent to discuss the matter with its parent company and to furnish any evidence in rebuttal of the presumption.</p> <p>10. the decision-maker will prepare a draft decision, setting out his/her proposed views in relation to whether or not an infringement has occurred and the corrective action proposed (where applicable)</p> <p>11. the draft is sent to the respondent and invites them to exercise their right to be heard within a specified timeframe</p> <p>12. upon receipt of the respondent's submissions, the decision-maker will finalise the draft, taking into account the respondent's views</p> <p>13. the draft will then be circulated via the IMI, to any concerned supervisory authorities</p> <p>14. the respondent will be provided with a copy of the final draft decision, for their information</p> <p>15. once the decision has exited the Article 60 process, it is adopted by the SA and is served on the respondent concerned.</p> <p>16. where the decision imposes a corrective fine, the SA must apply to the Court to have the fine confirmed before it can be enforced</p> <p>17. the required application cannot be made within the 28-day period following the service of the decision upon the respondent; this period of delay is to enable any of the parties concerned to file an appeal against the decision.</p> <p>18. once the fine has been confirmed by the Court, it may be enforced against the respondent</p>	
Italy	<ul style="list-style-type: none"> ▪ Procedure leading to an OSS decision: <ul style="list-style-type: none"> <u>LSA receiving a complaint:</u> <ol style="list-style-type: none"> 1. admissibility & possibility of amicable settlement 2. investigation + information sharing with CSAs 3. notification of DC/DP if corrective measures 4. approval & further adoption of a draft decision <u>LSA receiving a complaint from a CSA:</u> <ol style="list-style-type: none"> 1. admissibility & possibility of amicable settlement 2. investigation + information sharing with CSAs 3. notification of DC/DP if corrective measures 4. approval & further adoption of a draft decision <u>CSA receiving a complaint:</u> 	<ul style="list-style-type: none"> ▪ SA's practice

Member State/EEA State	NARs imposing steps or decisions pertaining to the OSS procedure	Origin of the rule (national legislation or SA's practice or interpretation)
	<ol style="list-style-type: none"> 1. admissibility & possibility of amicable settlement 2. information sharing with CSAs 3. approval of the draft decision 	
Latvia	<ul style="list-style-type: none"> ▪ No information 	<ul style="list-style-type: none"> ▪ No information
Liechtenstein	<ul style="list-style-type: none"> ▪ Procedure leading to an OSS decision: the SA will decide on the steps to take including the possibility of amicable settlement 	<ul style="list-style-type: none"> ▪ SA's practice
Lithuania	<ul style="list-style-type: none"> ▪ Procedure leading to an OSS decision: <ol style="list-style-type: none"> 1. investigation/inspection (all the parties are heard in written) 2. draft decision making [in case of fining (Art. 34 of LGPD)]: <ul style="list-style-type: none"> ➢ proposal to fine that is sent to the suspect ➢ hearing ➢ draft decision making 3. draft decision sent to CSAs 4. final decision approval 	<ul style="list-style-type: none"> ▪ SA's practice
Luxembourg	<ul style="list-style-type: none"> ▪ Procedure leading to an OSS decision: <ol style="list-style-type: none"> 1. search for amicable settlement 2. investigation 3. statement of objections 4. observations from DC/DP 5. decision on the investigation by the “<i>formation restreinte</i>” 6. in case of an OSS, draft decision sent to other SAs via IMI 7. final decision 	<ul style="list-style-type: none"> ▪ National legislation: Arts. 32, 37-41 of 2018 Act
Malta	<ul style="list-style-type: none"> ▪ First assessment of admissibility and determination of the course of the investigation 	<ul style="list-style-type: none"> ▪ SA's practice
Netherlands	<ul style="list-style-type: none"> ▪ Procedure leading to an OSS decision: <ol style="list-style-type: none"> 1. reception and assessment of complaint and its cross-border nature 2. closing of complaint / search of an alternative solution / start an investigation 3. advise on the appropriate measure including corrective measures 4. hearing (after sending the report of findings and the intention to impose corrective powers: cf. title 5.4.2 of the GALA) 5. draft decision shared with other SAs after the evaluation of the findings and the advice on the measure to impose and after hearing the parties but before a formal decision is taken and communicated to parties 	<ul style="list-style-type: none"> ▪ SA's practice
Norway	<ul style="list-style-type: none"> ▪ Procedure leading to an OSS decision: <ol style="list-style-type: none"> 1. fact finding 2. notification of the intent to make a decision 3. adoption of a decision (draft decision should be issued before the adoption of the decision) 	<ul style="list-style-type: none"> ▪ SA's practice except for the adoption of the decision (cf. Arts. 13-18 of the PAA)
Poland	<ul style="list-style-type: none"> ▪ Procedure leading to an OSS decision: <ol style="list-style-type: none"> 1. initiation of administrative proceedings 2. investigation 3. decision RE (1) initiation of administrative proceedings <ul style="list-style-type: none"> ▪ For cross-border cases the draft decision is submitted to other SAs after its notification to complainant and DC/DP to allow them to express their views on the evidence and materials collected and claims made (Art. 	<ul style="list-style-type: none"> SA's practice except on the initiation of the administrative proceedings (cf. Arts. 61-66, 77-81, 104-105 of the CAP)

Member State/EEA State	NARs imposing steps or decisions pertaining to the OSS procedure	Origin of the rule (national legislation or SA's practice or interpretation)
	<ul style="list-style-type: none"> 10(1) of the CAP) ▪ No mention to consult SAs in the national data protection act 	
Portugal	<ul style="list-style-type: none"> ▪ Procedure leading to an OSS decision (there is no specific provisions): <ol style="list-style-type: none"> 1. admissibility of the complaint 2. findings procedure 3. investigations 4. draft decision 5. shared with CSAs 6. draft decision sent to DCP/DP so as to give the right to be heard 7. final decision shared with CSAs to ascertain whether they agree with the final decision (concrete sanction to be imposed or not to impose a sanction at all) 	<ul style="list-style-type: none"> ▪ SA's practice
Romania	<ul style="list-style-type: none"> ▪ No information 	<ul style="list-style-type: none"> ▪ No information
Slovakia	<ul style="list-style-type: none"> ▪ Procedure leading to an OSS decision: <ol style="list-style-type: none"> 1. Complaint/petition/proceeding ex officio 2. Informing parties 3. Proceeding – collecting pieces of evidence for decision and their evaluation 4. Informing parties of the proceeding about evidence for decision before issuing a decision according to Art. 33(2) of the APA 5. Decision: during preliminary vetting the SA assesses if the case is cross border or not. If the case is cross border the SA applies Art. 99(4) of APDP 	<ul style="list-style-type: none"> ▪ SA's practice
Slovenia	<ul style="list-style-type: none"> ▪ The steps leading to an OSS decision should be interpreted in light of the GDPR and the national administrative rules: <ul style="list-style-type: none"> <u>INSPECTION procedure:</u> (Chapter VI of the Inspection Act): <ul style="list-style-type: none"> - Receiving a petition (complaint) or initiating the procedure ex officio - Performing specific investigative activities prior to the issuing of an inspection decision - Issuing a decision <u>ADMINISTRATIVE procedure:</u> <ul style="list-style-type: none"> - Receiving a petition (complaint against the refusal or rejection of DC to grant access or portability rights) - Establishing facts and circumstances - Adopting a decision 	<ul style="list-style-type: none"> ▪ SA's practice
Spain	<ul style="list-style-type: none"> ▪ Procedure leading to an OSS decision: <ol style="list-style-type: none"> 1. determine the national or cross-border nature of the data processing 2. admissibility of the complaint 3. preliminary investigation actions 4. decision to initiate the procedure to fine 5. provisional measures 	<ul style="list-style-type: none"> ▪ SA's practice
Sweden	<ul style="list-style-type: none"> ▪ No information 	<ul style="list-style-type: none"> ▪ No information

7.2 GENERAL TRENDS OBSERVED IN RELATION TO THE NATIONAL ADMINISTRATIVE RULES IMPOSING STEPS OR DECISIONS PERTAINING FOR THE OSS PROCEDURE

In most countries, there are no legal provisions setting up a specific procedure or specific steps or

decisions regarding the OSS mechanism. Furthermore, rules on when the CSAs should be consulted vary in the countries concerned.

As to the **specific steps** leading to an OSS decision, the following conclusions can be drawn:

1. In eleven countries, the procedure leading to an OSS decision is based upon SA's practice (or SA's interpretation of the procedure):
2. Belgium, Cyprus, Czech Republic, Estonia, France, Greece, Italy, Liechtenstein, Lithuania, Malta and Spain.
3. In four countries, the procedure leading to an OSS decision is based upon national data protection laws:
4. Bulgaria, Finland, Hungary and Luxembourg.
5. In four countries, the procedure leading to an OSS decision is based upon national data protection laws combined with national general administrative laws:
6. Germany, the Netherlands, Slovakia and Slovenia.
7. In three countries, the procedure leading to an OSS decision is based on national general administrative laws:
8. Estonia, Norway and Poland.
9. For two countries, we received the information that there are no specific legal provisions on the procedure leading to an OSS decision:
10. Austria and Portugal.

Regarding the **practical arrangements** between SAs in the context of an OSS procedure:

1. Informal arrangements between SAs:

In Bulgaria, arrangements with other SAs are made after deciding upon a complaint's admissibility and before examining the complaint's merits.

2. Discretionary decision of the SA

In Liechtenstein and Malta, the SAs will decide on the procedure (including the possibility of an amicable settlement, in Liechtenstein).

3. No consultation with other SAs before sharing draft decisions:

In Cyprus, there is no consultation with CSAs before sharing the draft decision.

4. Consultation or at least information of other SAs before the adoption of the draft decision

In France, the case is sent through IMI as soon as the cross-border processing is identified. Information is then shared with CSA before submitting a draft decision. CSAs may participate to the oral hearing of the parties.

In Italy, the SA shares information with other SAs after assessing the admissibility of the complaint and the possibility to reach an amicable settlement.

5. Sharing of the draft decision with the other SAs after its adoption

In Greece, the draft decision is shared with CSAs.

In Lithuania, the draft decision is sent to CSAs.

In Luxembourg, the draft decision is sent to the other SAs via IMI.

In the Netherlands, the draft decision is shared with other SAs after the assessment of the findings and the advice on the measure to be imposed and after hearing the parties, but this is before a formal decision is taken and communicated to the parties.

In Poland, the draft decision is shared with the other SAs after its notification to the complainant, controllers and processors to allow them to express their views on the evidence and materials collected and on the claims made against them. There is no formal indication on whether there is an obligation to consult with the other SAs.

In Portugal, the draft decision is shared with the CSAs. The final decision is shared with CSAs to ascertain whether they agree with the final decision.

7.3 QUESTIONS & CHALLENGES TO COOPERATION DUTIES STEMMING FROM THE APPLICATION OF NATIONAL ADMINISTRATIVE RULES IMPOSING STEPS OR DECISIONS TO THE OSS PROCEDURE

The procedure applied when handling an OSS case varies from country to country. There is no convergence nor harmonisation on any aspects of the OSS mechanism whatsoever. In some cases it could lead to a chaotic situation and a severe weakening of data protection in Europe regarding cross-border processing. It might also result in the breaching of the law's predictability, which is a fundamental right for controllers and processors and a fundamental legal principle in most of the Member States and in the European Union.

7.4 SUGGESTIONS AND POSSIBLE SOLUTIONS

The best solution seems to be to assess the possibility of drafting comprehensive Recommendations or Guidelines at the European (EDPB) level on the way to conduct an OSS procedure from the start, meaning starting with the identification of cross-border processing, then with the investigation phase, the information and consultation of SAs, the notification and hearing of the parties, the decision-making procedure, and the legal effects of the decisions adopted during the OSS procedure – based upon SAs' practices and legal constraints.

8 CONCLUSION

It appears that all SAs have to comply with national general administrative rules when carrying out their cooperation duties in the context of an OSS procedure. Those national general administrative rules might be applicable to all kinds of administrative proceedings. They are not necessarily specific or adapted to the OSS procedure. This does not imply in itself that they are not compatible with the OSS procedure. In addition to those national general administrative rules, a large majority of countries have passed some specific rules regarding how to organise their cooperation duties in the context of an OSS procedure. As a general rule, these specific rules only partially cover aspects of the OSS mechanism. A minority of countries have passed more comprehensive national administrative rules regarding the OSS mechanism. Some SAs have expressly indicated that national administrative rules should be interpreted and applied in light of the rules laid down by the GDPR. There are other general trends between the national administrative rules applicable to cooperation duties. In nearly all the countries, time limits or deadlines are suspended or may be extended in case of an OSS procedure.

In a large majority of countries, complaints must comply with requirements laid down by national administrative rules (e.g. formal requirements including the identification of the complainant, prior exercise of data subject's rights, damages, substantiation of the complaint, language requirements or deadlines). Failing to meet these requirements might lead to the (early) dismissal of the complaint - but not always.

A vast majority of countries recognise the controllers' and processors' fundamental right to be heard - especially in view of imposing an administrative fine or exercising corrective powers. They also recognise, to some extent, the obligation to provide information on the proceedings to the complainant and/or the controller or processor. However, there is no unanimity on the moment when the hearing or information should occur.

A substantial number of countries recognise the possibility of amicable settlements between the complainant and the controller or processor.

There is usually an obligation to inform the parties on the opening of the case and of the procedure, on the investigation and its outcomes, on the exercise of corrective powers and on the decisions taken (including draft decisions and final decisions).

There are no harmonised rules as to whether a draft decision or any other decision is needed when an investigation is halted mid-procedure or when the complaint is withdrawn by the complainant or is deemed withdrawn (e.g. the controller or processor have implemented the corrective measures imposed by the SA) and whether and when this information should be shared with the other SAs. The same applies for amicable settlements.

Some SAs have stressed the lack of legal provisions to conduct joint operations. However, in some countries, this issue is addressed by some national administrative rules. It must be stressed that it appears that sometimes, a SA may not rely on the investigation performed by another SA to ground its decisions for legal reasons (in other words the outcome of the investigation might not be legally admissible in another country).

The OSS procedure also raises the difficult question of the enforcement of the decision passed by one SA in another country.

In view of the findings of the study, a first short-term solution could be to assess the possibility of issuing Recommendations or Guidelines for each of the six topics covered by the analysis, in order to maximise the possibility of solving this at EDPB level. In the long run, a more global solution could consist of the drafting of comprehensive Recommendations or Guidelines at European level (EDPB) on the way to conduct an OSS procedure from the start, meaning starting with the identification of cross-border processing, then with the investigation phase, the information and consultation of the SAs, the notification and hearing of the parties, the decision-making procedure, and the legal effects of the decisions adopted during the OSS procedure. It would be important to assess the limitations of a harmonised solution, due to divergences, not only of SAs practices, but also of national laws. If the work

of the EDPB faces this limitation, it would be important to make a legal assessment of the legal possibility to call for more harmonised rules on this topic.

ANNEX 1 – QUESTIONNAIRE FOR THE NATIONAL SUPERVISORY AUTHORITIES

QUESTIONNAIRE – General information about national rules impacting the cooperation duties

Questions related to the main data protection law

1. What is the main piece(s) of legislation that have been adopted by your Member State to adapt national legislation to the GDPR – e.g. national legal provisions adopted or amended to adapt the national data protection law to the GDPR, for the enforcement of the GDPR or applicable for the enforcement of the GDPR duties in the matter of cooperation?

Please provide reference to the main piece(s) of national legislation that have been enacted and/or amended to adapt national data protection law to the GDPR, for the enforcement of the GDPR or applicable for the enforcement of the GDPR duties in the matter of cooperation. Please provide us a copy of such relevant law(s) as well as an English translation if available.

2. Which provisions of this law(s) your organisation has to comply with while fulfilling cooperation duties under the one-stop-shop (OSS) mechanism for the EEA States, as set out in Articles 56 and 60 of the GDPR?

Please quote the main provisions of this legislation, applicable to EEA OSS mechanism duties under the GDPR.

3. Which provisions of this law(s) your organisation has to comply with while carrying out preparatory acts which could lead to the one-stop-shop mechanism, as set out in Articles 56 and 60 of the GDPR (i.e. while carrying out investigations or handling complaints)?

Please quote the main provisions of this legislation, applicable to the acts which could lead to the one-stop-shop mechanism (in the context of investigations, handling of complaints, etc.).

Questions related to other laws setting out administrative rules

4. Apart from this legal act(s), what are the other pieces of legislation that you are obliged to apply while performing your tasks BEFORE and DURING the one-stop-shop mechanism in the GDPR?

Please provide reference to these other legal acts. Please provide us a copy of the relevant sections as well as an English translation if available.

Questions related to the application of national administrative rules to GDPR cooperation and the one-stop-shop mechanism

5. Please describe the different steps of your procedure provided by your national law(s) leading to any OSS decision(s).

Please provide reference to these national legal act(s). Please provide us a copy of the relevant sections as well as an English translation if available. If exist, please also provide to us any scheme of such procedure / different national steps that lead to any OSS decision(s).

6. In particular, please describe **what are the provisions of national law(s)** (either data protection, administrative or other) that you are obliged to apply with respect to the following aspects?

In the boxes below, please provide a short explanation as well as a reference to the legislation setting out the relevant administrative rules. Please also quote (in full) from these laws the relevant provisions which apply to the different aspects. Please provide us a copy of the relevant sections as well as an English translation if available. Do not hesitate to provide short explanations. If there is no specific legal duty but the matter is left to your appreciation, please indicate it clearly.

- **Timing/deadline** within which a complaint or investigation should be handled:

- **Grounds** (other than the ground provided in Article 57(4) of the GDPR referring to manifestly unfounded or excessive requests) for deciding on the admissibility of complaints received from individuals:

- Obligation for your organisation to notify the data controller/processor of a **forthcoming investigation** or the **forthcoming exercise of corrective powers**. If such prior notification obligation exists under the national law, please specify in the box below, if your national law specify whether these should take place prior to the consultation of the other supervisory authorities (SAs) on the draft decision:

- **The moment in the procedure** when **the draft decision** (Article 60.3 GDPR) has to be shared with the other concerned supervisory authorities. Please also describe at which step of the procedure provided by your national law this should happen:

- **The moment(s)** during this procedure when the **duty to hear the parties concerned will apply**. Please specify if this should, according to your national legal framework, take place before consulting the other concerned SAs:

- Any other provisions regulating your organisation's investigative powers which might have an implication on the fulfilment of cooperation duties by your organisation:

ANNEX 2 – LIST OF STAKEHOLDERS CONTACTED

Supervisory authorities of the 27 EU Member States of the European Union and the 3 EFTA-EEA States have been contacted with the help of the EDPB Secretariat.

Table 7: List of competent SAs

Member State	Competent SA
Austria	<i>Österreichische Datenschutzbehörde</i>
Belgium	<i>Autorité de la protection des données/Gegevensbeschermingsautoriteit (APD/GBA)</i>
Bulgaria	Commission for Personal Data Protection
Croatia	Croatian Personal Data Protection Agency
Cyprus	Commissioner for Personal Data Protection
Czech Republic	Office for Personal Data Protection
Denmark	<i>Datatilsynet</i>
Estonia	Estonian Data Protection Inspectorate - <i>Andmekaitse Inspektsioon</i>
Finland	Office of the Data Protection Ombudsman
France	<i>Commission Nationale de l'Informatique et des Libertés (CNIL)</i>
Germany	<i>Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit and several Landesdatenschutzbeauftragte</i>
Greece	Hellenic Data Protection Authority
Hungary	Hungarian National Authority for Data Protection and Freedom of Information
Iceland	The Data Processing Authority - <i>Persónuvernd</i>
Ireland	Data Protection Commission (DPC)
Italy	<i>Garante per la protezione dei dati personali</i>
Latvia	Data State Inspectorate
Liechtenstein	<i>Datenschutzstelle</i>
Lithuania	State Data Protection Inspectorate
Luxembourg	<i>Commission Nationale pour la Protection des Données (CNPD)</i>
Malta	Office of the Information and Data Protection Commissioner
Netherlands	<i>Autoriteit Persoonsgegevens</i>
Norway	Norwegian Data Protection Authority - <i>Datatilsynet</i>
Poland	Personal Data Protection Office - <i>Urząd Ochrony Danych Osobowych</i>
Portugal	<i>Comissão Nacional de Proteção de Dados (CNPD)</i>
Romania	The National Supervisory Authority for Personal Data Processing
Slovakia	Office for Personal Data Protection of the Slovak Republic
Slovenia	Information Commissioner of the Republic of Slovenia
Spain	<i>Agencia Española de Protección de Datos (AEPD)</i>
Sweden	<i>Datainspektionen</i>

ANNEX 3 – SOURCES OF INFORMATION

Legal documents at EU level

Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391–407 and OJ C 326, 26.10.2012, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT>.

Directive (EU) 2019/1 of the European Parliament and of the Council of 11 December 2018 to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88.

Other literature at EU level

Article 29 Data Protection Working Party, Guidelines for identifying a controller or processor's lead supervisory authority (WP 244 rev.01), adopted on 13 December 2016, last revised and adopted on 5 April 2017.

Cooperation and consistency? Nine months in, the EDPB reflects on GDPR, 5 April 2019, accessible at: <https://www.technologylawdispatch.com/2019/04/privacy-data-protection/cooperation-and-consistency-nine-months-in-the-edpb-reflects-on-gdpr/>.

Council of the EU: Communication from the Commission to the European Parliament pursuant to Article 294(6) of the Treaty on the Functioning of the European Union concerning the position of the Council on the adoption of a Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and repealing Directive 95/46/EC, COM(2016) 214 final, brussels, 12 April 2016.

EDPB: Cross-border cooperation and consistency procedures – State of play, 20 July 2018, accessible at: https://edpb.europa.eu/news/news/2018/cross-border-cooperation-and-consistency-procedures-state-play_en.

EDPB: European Data Protection Board – Second plenary meeting: ICANN, PSD2, Privacy Shield, 5 July 2018, accessible at: https://edpb.europa.eu/news/news/2018/european-data-protection-board-second-plenary-meeting-icann-psd2-privacy-shield_en.

EDPB: First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities.

EDPB: Graphs demo, 22 May 2019, accessible at: https://edpb.europa.eu/graphs-demo_en.

EDPB: Opinion 8/2019 on the competence of a supervisory authority in case of a change in circumstances relating to the main or single establishment, 9 July 2019.

EDPB: The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC, 21 January 2019, accessible at: https://edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_sl.

European Union Agency for Fundamental Rights and Council of Europe, 2018, Handbook on European data protection law, 2018 edition, Publications Office of the European Union, Luxembourg.

Guidelines for identifying a controller or processor's lead supervisory authority, wp244rev.01.

How Are European Supervisory Authorities Exercising Cooperation and How Are European Supervisory Authorities Exercising Cooperation and Consistency In Practice?, 2 September 2019, accessible at: <https://www.globalprivacyblog.com/gdpr/how-are-european-supervisory-authorities-exercising-cooperation-and-consistency-in-practice/>

exercising-cooperation-and-consistency-in-practice/.

Recap: EDPB's first-year review of GDPR, 21 March 2019, accessible at: <https://iapp.org/news/a/recap-edpbs-first-year-review-of-the-gdpr/>.

What happened to the one-stop shop?, 21 February 2019, accessible at: https://wp.nyu.edu/compliance_enforcement/2019/04/15/gdpr-what-happened-to-one-stop-shop-enforcement/.

Member States' national data protection laws passed to implement the GDPR and national administrative rules applicable to the OSS mechanism

Table 8: Overview of national laws

Member State	National data protection laws	NARs applicable to the OSS mechanism
Austria	<ul style="list-style-type: none"> ▪ Federal Act concerning the Protection of Personal Data (DSG), accessible at: https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.html 	<ul style="list-style-type: none"> ▪ General administrative Procedure Act (GAPA)
Belgium	<ul style="list-style-type: none"> ▪ 30 July 2018 - Act on the protection of natural persons with regard to the processing of personal data (2018 Act) ▪ 3 December 2017 - Act establishing the Data Protection Authority (2017 Act) 	<ul style="list-style-type: none"> ▪ General Principles of Good Administration
Bulgaria	<ul style="list-style-type: none"> ▪ Personal Data Protection Act (PDPA), accessible at: https://www.cpdp.bg/en/index.php?p=element&aid=1194 ▪ Rules on the activity of the Commission for Personal Data Protection and its administration, accessible at: https://www.cpdp.bg/en/index.php?p=element&aid=36 	<ul style="list-style-type: none"> ▪ Administrative Procedural Code (APC) ▪ Administrative Infringements and Sanctions Act
Croatia	<ul style="list-style-type: none"> ▪ Law on Implementation of the General Data Protection Regulation (OG 42/18) (LoIoGDPR) 	<ul style="list-style-type: none"> ▪ Law on Administrative Procedure
Cyprus	<ul style="list-style-type: none"> ▪ Law 125(I)/2018 for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data, accessible at: http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/2B53605103DCE4A4C225826300362211/\$file/Law%20125(I)%20of%202018%20ENG%20final.pdf 	<ul style="list-style-type: none"> ▪ General Principles of Administrative Law
Czech Republic	<ul style="list-style-type: none"> ▪ Act No. 110/2019 Coll., on personal data processing of 12 March 2019, accessible at: https://www.uouo.cz/en/vismo/zobraz_dok.asp?id_org=200156&id_ktg=1420&archiv=0&p1=1105 ▪ Act No. 111/2019 Coll 	<ul style="list-style-type: none"> ▪ Administrative Procedure Code (APC) ▪ Inspection Act (No 255/2012) ▪ Liability for Administrative Delicts and Related Proceedings Act (No 250/2016)
Denmark	<ul style="list-style-type: none"> ▪ Danish Data Protection Act (2018), accessible at: https://www.datatilsynet.dk/media/6894/danish-data-protection-act.pdf 	<ul style="list-style-type: none"> ▪ Danish Public Administration Act ▪ Danish Access to Public Administration Files Act
Estonia	<ul style="list-style-type: none"> ▪ Personal Data Protection Act of 12 December 2018 (PDPA) 	<ul style="list-style-type: none"> ▪ Administrative Procedure Act ▪ Law Enforcement Act ▪ Code of Civil Procedure ▪ Code of Misdemeanour Procedure
Finland	<ul style="list-style-type: none"> ▪ Data Protection Act 2018 (DPA), accessible at: https://www.finlex.fi/en/laki/kaannokset/2018/en20181050.pdf 	<ul style="list-style-type: none"> ▪ Administrative Procedure Act (434/2003)
France	<ul style="list-style-type: none"> ▪ Act No 78-17 of 6 January 1978 on Informatics, Files and Liberties (LIL Act), accessible at: 	<ul style="list-style-type: none"> ▪ Constitution, Art. 2 ▪ Code of relationships

Member State	National data protection laws	NARs applicable to the OSS mechanism
	<p>https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460</p> <ul style="list-style-type: none"> ▪ Decree No 2019-536 of 29 May 2019 implementing act of 6 January 1978, accessible at: https://www.legifrance.gouv.fr/eli/decret/2019/5/29/JUSC1911425D/jo/texte (Decree) ▪ <i>Règlement intérieur de la CNIL</i> (CNIL RoI), accessible at: https://www.cnil.fr/fr/reglement-interieur-de-la-cnil 	<ul style="list-style-type: none"> ▪ between the public and the administration, Art. L211-2 ▪ Law on Administrative Procedure OG 47/09, Art. 101
Germany	<ul style="list-style-type: none"> ▪ Federal Data Protection Act (<i>Bundesdatenschutzgesetz</i> - BDSG), accessible at: https://www.gesetze-im-internet.de/englisch_bdsge/englisch_bdsge.pdf ▪ Baden-Wuerttemberg State Data Protection Act ▪ Lower Saxony Data Protection Act ▪ Act transposing Directive (EU) 2016/680 (Saxony-Anhalt Data Protection Directive Implementation Act – DSUG LSA) Of 2 August 2019 ▪ <i>Thüringer Datenschutzgesetz</i> 	<ul style="list-style-type: none"> ▪ Federal Administrative Procedures Act (<i>Verwaltungsverfahrensgesetz</i> - VwVfG) ▪ Act on Regulatory Offences ▪ Federal Code of Criminal Procedure ▪ <i>Thüringer Verwaltungsverfahrensgesetz</i> ▪ <i>Thüringer Verwaltungszustellungs- und Vollstreckungsgesetz</i> ▪ Saxony-Anhalt Administrative Procedure Act (VwVfG LSA) Of 18 November 2005
Greece	<ul style="list-style-type: none"> ▪ Law 4624/2019, aiming both at the enforcement of the GDPR and the enforcement of the GDPR duties in the matter of cooperation 	<ul style="list-style-type: none"> ▪ Code of Administrative Procedure (Law 2690/99)
Hungary	<ul style="list-style-type: none"> ▪ Act CXII of 2011 on the right to informational self-determination and on the freedom of information ▪ Act XIII of 2018 designating the Hungarian Data Protection and Freedom of Information Agency as Hungary's GDPR supervisory authority ▪ Act XLVII of 1997 on the processing and protection of personal data concerning health (the 'Health Data Processing Act') 	<ul style="list-style-type: none"> ▪ General Procedural Rules ▪ Act CL of 2016 of the Code of General Administrative Procedure (CGAP)
Iceland	<ul style="list-style-type: none"> ▪ Act No. 90/2018 on Data Protection and the Processing of Personal Data of 27 June 2018 	<ul style="list-style-type: none"> ▪ Administrative Procedures Act (APA)
Ireland	<ul style="list-style-type: none"> ▪ Data Protection Act 2018 and Regulations 2018 (S.I. No. 314 of 2018) (S.I. No. 188 of 2019) ▪ Data Sharing and Governance Act 2019 ▪ S.I. 222/2019 – Circuit Court Rules (Data Protection Actions) 2019 together with Orders 60 and 64B of the Circuit Court Rules 	<ul style="list-style-type: none"> ▪ Bunreacht na hÉireann (the Constitution of Ireland) ▪ Irish Administrative Law ▪ Case law of England and Wales ▪ European Convention on Human Rights Act, 2003 ▪ Interpretation Act, 2005 ▪ Administrative Procedure Act No 37/1993 (Art. 10 on investigations)
Italy	<ul style="list-style-type: none"> ▪ Italian Data Protection Code (Containing provisions to adapt the national legislation to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and 	<ul style="list-style-type: none"> ▪ Law No 689/1981 on the application of administrative fines ▪ Law No 241/1990 on the Administrative Procedure

Member State	National data protection laws	NARs applicable to the OSS mechanism
	<ul style="list-style-type: none"> ▪ repealing Directive 95/46/EC (IDPC) ▪ Regulation on internal procedures with an external relevance intended to carry out the tasks and exercise the powers conferred on the <i>Garante per la protezione dei dati personali</i>, and with a view to the adoption of corrective measures and administrative fines (Section 142(5), Section 154 (1)(b) and (3), Section 156 (3)(a) and Section 166(9), Legislative Decree No 196 of 30 June 2003 (“Italian Data Protection Code”), as amended by Legislative Decree No 101 of 10 August 2018) ▪ “Rules of Procedure No 1/2019” by the Italian Data Protection Authority (RoP) 	<p>Act</p> <ul style="list-style-type: none"> ▪ Italian FOIA Law: Legislative decree No 33/2013 as amended by legislative decree No 97/2016 ▪ Legislative Decree No 196/2003
Latvia	<ul style="list-style-type: none"> ▪ Personal Data Processing Law, 132 (6218), 4 July 2018 (PDP Law) 	<ul style="list-style-type: none"> ▪ Administrative Procedure Law (APL) ▪ Administrative Violations Code (cf. Division IV on Administrative Infringement Proceedings) ▪ Law on Submissions
Liechtenstein	<ul style="list-style-type: none"> ▪ Data Protection Act of 4 October 2018 (DPA) ▪ Data Protection Ordinance of 4 October 2018 	<ul style="list-style-type: none"> ▪ Law on Administrative Procedure (LVG)
Lithuania	<ul style="list-style-type: none"> ▪ Law on Legal Protection of Personal Data (LGPD), accessible at: https://www.e-tar.lt/portal/legalAct.html?documentId=43cddd8084cc11e8ae2bfd1913d66d57 	<ul style="list-style-type: none"> ▪ Law on Public Administration ▪ Administrative Offences Code
Luxembourg	<ul style="list-style-type: none"> ▪ Act of 1 August 2018 on the organisation of the National Data Protection Commission, implementing Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), amending the Labour Code and the amended Act of 25 March 2015 stipulating the rules of remuneration and the terms and conditions for the promotion of State civil servants (2018 Act) ▪ Regulation of the National Data Protection Commission on the investigation procedure, Adopted by Decision No 4AD/2020 of 22.01.2020, pursuant to Art. 40 of the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework (Regulation) ▪ Rules of Procedure of the National Data Protection Commission Adopted by Decision No 3/2020 of 22.01.2020, pursuant to Art. 32 (1) and 33 of the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework (Act of 1 August 2018) 	<ul style="list-style-type: none"> ▪ Law of 1 December 1978 governing the non-contentious administrative procedure ▪ Loi du 7 novembre 1996 portant organisation des juridictions de l'ordre administratif ▪ Grand-Ducal Regulation of 8 June 1979 on the procedure to be followed by the State or municipal administrative authorities
Malta	<ul style="list-style-type: none"> ▪ Data Protection Act, CAP 586, accessible at: http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=12839&l=1 ▪ Subsidiary legislation 586.08 Data Protection (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), accessible at: https://idpc.org.mt/en/Legislation/SL%20586.08.pdf ▪ Subsidiary legislation 586.09 Restriction of the Data Protection (Obligations and Rights), accessible at: https://idpc.org.mt/en/Legislation/SL%20586.09.pdf ▪ Subsidiary legislation 586.10 Processing of Data concerning Health for Insurance Purposes, accessible at: 	

Member State	National data protection laws	NARs applicable to the OSS mechanism
	<ul style="list-style-type: none"> ▪ https://idpc.org.mt/en/Legislation/SL%20586.10.pdf ▪ Subsidiary legislation 586.11 Processing of Child's Personal Data in Relation to the Offer of Information Society Services, accessible at: https://idpc.org.mt/en/Legislation/SL%20586.11.pdf 	
Netherlands	<ul style="list-style-type: none"> ▪ Act of 16 May 2018 containing rules for the implementation of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016, L 119) (General Data Protection Regulation Implementation Act) (2018 Act) ▪ Adaptation Act General Data Protection Regulation ▪ <i>Uitvoeringswet Algemene verordening gegevensbescherming</i> ▪ <i>Beleidsregels openbaarmaking door de Autoriteit Persoonsgegevens</i> 	<ul style="list-style-type: none"> ▪ General Administrative Law Act (GALA) ▪ Framework Act on Independent Administrative Authorities ▪ <i>Beleidsregels Prioritering klachtenonderzoek</i>
Norway	<ul style="list-style-type: none"> ▪ <i>Lov 15. juni 2018 nr. 38 om behandling av personopplysninger</i> (Personal Data Act), accessible at: https://lovdata.no/dokument/NL/lov/2018-06-15-38 	<ul style="list-style-type: none"> ▪ Public Administration Act (PAA) ▪ Freedom of Information Act
Poland	<ul style="list-style-type: none"> ▪ Act of 10 May 2018 on the Protection of Personal Data, accessible at: https://uodo.gov.pl/en/file/307 ▪ Act of 21 February 2019 amending certain acts in connection with ensuring the application of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) 	<ul style="list-style-type: none"> ▪ Code of Administrative Procedure (CAP) ▪ 2002 Act on Proceedings before Administrative Courts ▪ 2018 Law on Entrepreneurs (cf. Art. 55)
Portugal	<ul style="list-style-type: none"> ▪ Law 58/2019, of 8th of August ▪ DELIBERAÇÃO/2019/494, adopted at the plenary meeting of <i>Comissão Nacional de Proteção de Dados</i> (CNPD) on 3 September 2019 	<ul style="list-style-type: none"> ▪ National Organisation Law (Law 43/2001) ▪ National Fining Regime
Romania	<ul style="list-style-type: none"> ▪ The law on implementing measures of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ▪ The Law amending and supplementing Law no. 102/2005 on the establishment, organisation and functioning of the National Supervisory Authority for Personal Data Processing, and repealing Law No. 677/2001 on the protection of individuals with regard to the processing of personal data and on the free movement of such data 	
Slovakia	<ul style="list-style-type: none"> ▪ Act No. 18/2018 on Personal Data Protection and amending and supplementing certain Acts (APDP), accessible at: https://dataprotection.gov.sk/uouu/en/content/national-legislation 	<ul style="list-style-type: none"> ▪ Administrative Proceeding Act No 71/1967 (APA)
Slovenia	<ul style="list-style-type: none"> ▪ Personal Data Protection Act (not adapted to GDPR) 	<ul style="list-style-type: none"> ▪ Information Commissioner Act ▪ Inspection Act ▪ General Administrative Procedure Act ▪ Minor Offences Act ▪ Decree on Administrative Operations

Member State	National data protection laws	NARs applicable to the OSS mechanism
Spain	<ul style="list-style-type: none"> ▪ Organic Law 3/2018 of 5 December 2018 (OL 3/2018) 	<ul style="list-style-type: none"> ▪ General Rules on Administrative Procedures (on a supplementary basis)
Sweden	<ul style="list-style-type: none"> ▪ Data Protection Act (SFS 2018:218 <i>Lag med kompletterande bestämmelser till EU:s dataskyddsförordning</i>), accessible at: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2018218-med-kompletterande-bestämmelser_sfs-2018-218 ▪ The Swedish Data Protection Regulation (2018:219), accessible at: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-2018219-med-kompletterande_sfs-2018-219 ▪ Ordinance (2007:975) on Instructions for the Swedish Data Protection Authority 	<ul style="list-style-type: none"> ▪ General Administration Laws ▪ Normal Procedural Rules ▪ Supervision Policy

Other sources of information (questionnaires)

Report commissioned by the European Commission on the evaluation of the GDPR (only the part concerning Chapter VII).

Results from the EDPB questionnaire regarding “Amicable settlements”.

Results from the EDPB questionnaire regarding the investigation of complaints (only the part on the sharing of information before submitting a draft decision).

ANNEX 4 - ACRONYMS AND ABBREVIATIONS

The table hereunder provides a list of acronyms and abbreviations used throughout this study.

Table 9: Acronyms and abbreviations

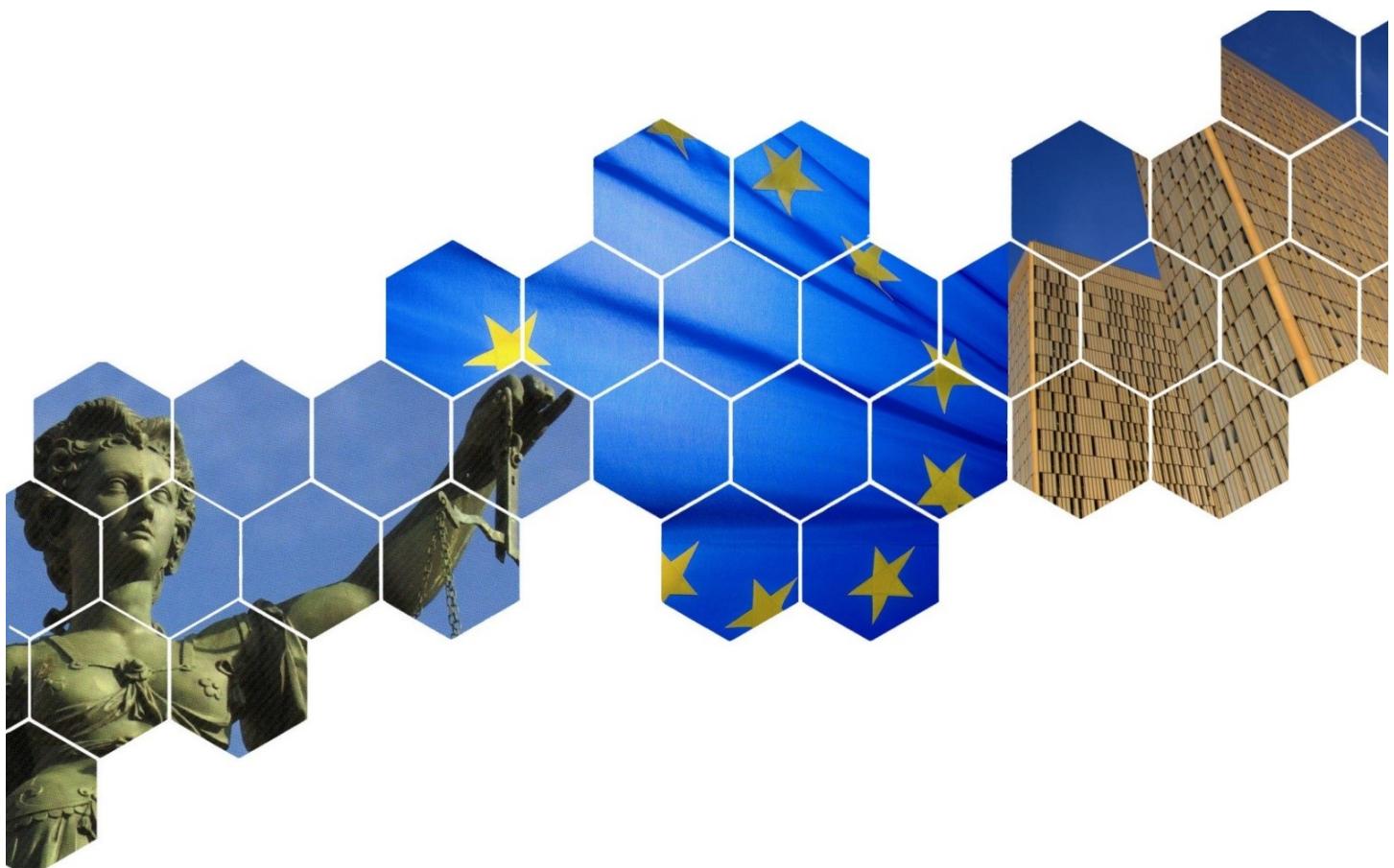
Acronym and abbreviation	Explanation
AEPD	<i>Agencia Española de Protección de Datos</i> (Spanish SA)
APA	Icelandic Administrative Procedures Act Slovakian Administrative Proceeding Act
APC	Bulgarian Administrative Procedural Code Czech Administrative Procedure Code
APD/GBA	<i>Autorité de la protection des données/Gegevensbeschermingsautoriteit</i> (Belgium SA)
APDP	Slovakian Act No. 18/2018 on Personal Data Protection and amending and supplementing certain Acts
APL	Latvian Administrative Procedure Law
BDSG	German Federal Data Protection Act - <i>Bundesdatenschutzgesetz</i>
CAP	Polish Code of Administrative Procedure
CGAP	Hungarian Act CL of 2016 of the Code of General Administrative Procedure
CNIL	<i>Commission Nationale de l'Informatique et des Libertés</i> (French SA)
CNIL Rol	French <i>Règlement intérieur de la CNIL</i>
CNPD	<i>Commission Nationale pour la Protection des Données</i> (Luxembourg SA) <i>Comissão Nacional de Proteção de Dados</i> (Portuguese SA)
CSA	Concerned Supervisory Authority
DC	Controller
Decree	French Decree No 2019-536 of 29 May 2019 implementing act of 6 January 1978
DP	Processor
DPA	Finish Data Protection Act Liechtenstein Data Protection Act of 4 October 2018
DPC	Data Protection Commissioner (Irish SA)
DS	Data Subject
DSG	Austrian Federal Act concerning the Protection of Personal Data
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EEA	European Economic Area
EFTA	European Free Trade Association
EU	European Union
GALA	Dutch General Administrative Law Act
GAPA	Austrian General administrative Procedure Act

GDPR	General Data Protection Regulation
IDPC	Italian Data Protection Code
LGPD	Lithuanian Law on Legal Protection of Personal Data
LIL Act	French Act No 78-17 of 6 January 1978 on Informatics, Files and Liberties
LoIoGDPR	Croatian Law on Implementation of the General Data Protection Regulation
LSA	Lead Supervisory Authority
LVG	Liechtenstein Law on Administrative Procedure (LVG)
NAR	National Administrative Rules
OL 3/2018	Spanish Organic Law 3/2018 of 5 December 2018 (OL 3/2018)
OSS	One-Stop-Shop Mechanism
PAA	Norwegian Public Administration Act
PDP Law	Latvian Personal Data Processing Law
PDPA	Bulgarian Personal Data Protection Act Estonian Personal Data Protection Act
Regulation	Luxembourg Regulation of the National Data Protection Commission on the investigation procedure, Adopted by Decision No 4AD/2020 of 22.01.2020, pursuant to Art. 40 of the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework
RoP	Rules of Procedure No. 1/2019 by the Italian Data Protection Authority
SA	Supervisory Authority
VwVfG	German Federal Administrative Procedures Act - <i>Verwaltungsverfahrensgesetz</i>

Study on the enforcement of GDPR obligations against entities established outside the EEA but falling under Article 3(2) GDPR

Final Report

Specific contract No. 2020-1103 (EDPS/2019/02-09)



November 2021

This study has been prepared by Milieu under Contract No 2020-1103 (EDPS/2019/02-09) for the benefit of the EDPB.



The study has been carried out by researchers of the Centre de recherche, Information, Droit et Société (CRIDS) at University of Namur (Belgium), with the support of researchers from Milieu Consulting SRL. The leading author of the study report is Jean Hervege (CRIDS).

The information and views set out in this study are those of the author(s) and do not reflect the official opinion of the EDPB. The EDPB does not guarantee the accuracy of the data included in this study. Neither the EDPB nor any person acting on the EDPB's behalf may be held responsible for the use which may be made of the information contained therein.

Milieu Consulting SRL, Chaussée de Charleroi 112, B-1060 Brussels, tel.: +32 2 506 1000; e-mail: EDPB.legalstudies@milieu.be; web address: www.milieu.be.

**Study on the enforcement of GDPR obligations against entities established outside
the EEA but falling under Article 3(2) GDPR**

TABLE OF CONTENT

EXECUTIVE SUMMARY.....	5
1 INTRODUCTION.....	8
1.1 Research questions and scope of the Study	8
1.2 Methodology	8
1.3 Report outline	9
2 LEGAL ANALYSIS.....	10
2.1 Possibility to summon a third-country controller/processor.....	10
2.1.1 Summary of SA responses.....	10
2.1.2 Consequences of Case C-645/19 on the interpretation of Article 58(5) of the GDPR	12
2.1.3 Key findings.....	15
2.2 Analysis of enforcement of SAs' investigative and corrective powers in California, the UK and China	15
2.2.1 First preliminary remark: The nature of SAs' investigative and corrective powers.....	15
2.2.2 Second preliminary remark: The possibility to exercise SAs' investigative and corrective powers beyond the EEA territories ...	18
2.2.3 The enforcement of SAs' investigative and corrective powers in California.....	20
2.2.4 The enforcement of SAs' investigative and corrective powers in the UK	26
2.2.5 The enforcement of SAs' investigative and corrective powers in China	29
2.3 Identification of legal instruments that could support enforcement of the GDPR.....	31
2.3.1 Legal instruments identified by SAs	31
2.3.2 Other instruments to consider	32
2.3.3 Key findings.....	33
2.4 Sharing SAs' experiences and identification of other types of actions	33
2.4.1 Sharing SAs' experiences.....	33
2.4.2 Identification of other types of action and SAs' observations	36
2.4.3 Key findings.....	37
2.5 Analysis of the possibility to rely on unilateral commitments from controllers/processors in the matters of choice of jurisdiction and applicable law	37
2.5.1 Possibility for an agreement between controllers/processors and SAs on choice of jurisdiction.....	37
2.5.2 Possibility to rely on a choice of jurisdiction in BCR	38
2.5.3 Possibility to rely on a choice of jurisdiction in a unilateral commitment from controllers/processors	38
2.5.4 Possibility for an agreement between controllers/processors and SAs on choice of the applicable law	38
2.5.5 Possibility to rely on a choice of applicable law in BCR.....	38
2.5.6 Possibility to rely on choice of applicable law in a unilateral commitment from controllers/processors	38

2.5.7	Impact of CJEU interpretation of the notion of 'civil and commercial matters'	39
2.5.8	Key findings.....	39
2.6	Importance of controller/processor representatives.....	39
2.6.1	Added value of controller/processor representatives in the experience of SAs	39
2.6.2	Limits to the added value of controller/processor representatives as perceived by SAs	40
2.6.3	SAs' experiences of controller/processor representatives.....	40
2.6.4	Legal analysis of the scope of representatives' obligations under the GDPR.....	40
2.6.5	Key findings.....	43
2.7	International cooperation foreseen in the GDPR (Article 50).....	43
2.7.1	Main obstacles to international cooperation in the field of data protection identified by SAs	43
2.7.2	Tools to improve international cooperation in the field of data protection identified by SAs	44
2.7.3	Identification of third countries that would cooperate on data protection and/or recognise SAs' investigative or corrective powers.....	44
2.7.4	MoUs	44
2.7.5	Enforcement of SA investigative and corrective powers in EU trade agreements	45
2.7.6	Key findings.....	45
3	CONCLUSIONS	46
ANNEX 1 - QUESTIONNAIRE		49
ANNEX 2 – SOURCES OF INFORMATION		60
ANNEX 3 - ACRONYMS AND ABBREVIATIONS		65

EXECUTIVE SUMMARY

This Study analyses the possibilities available to enforce Supervisory Authorities' (SAs) investigative and corrective powers against third-country controllers or processors that fall under the scope of Article 3(2) of the General Data Protection Regulation (GDPR), but are not willing to cooperate and did not designate a representative in the European Economic Area (EEA) or the European Union (EU). The analysis focuses on controllers and processors established in California (United States of America, US) and in the United Kingdom (UK). Where possible, the Study provides information on the possibility to enforce these powers against those controllers and processors established in the People's Republic of China (China).

Two main research methods were used: desk research (review of legal literature, national, European and international legal instruments and case-law) and collection of information through a questionnaire sent to the SAs.

The main findings are as follows.

1. Possibility to summon a third-country controller/processor to appear before the SA's Office or its county court

There are some differences between SAs' powers to summon a third-country controller/processor to appear before the SA's Office or in a Court of the SA's country. They are uncertainties as to the possibility for SAs to initiate legal proceedings in another EU Member States or in a third country on the basis of Article 58(5) of the GDPR. The Court of Justice of the European Union (CJEU) case-law is unclear as to whether it could accept to recognise the jurisdiction of a Member State on the basis of Article 58(5) of the GDPR when the controller/processor has no establishment on the territory of any EU Member State.

2. Analysis of the enforcement of SAs' investigative and correctives powers in California, the UK and in China

SAs do not qualify as 'courts or tribunals' in the meaning of Article 267 of the Treaty on the Functioning of the European Union (TFEU) when exercising their investigative and corrective powers and SAs should be considered as exercising 'public powers' under European law when making use of special powers that go beyond those arising from the ordinary legal rules applicable to relationships between private individuals. With respect to this, the wording of Article 58 GDPR might be slightly misleading in respect of the nature of these powers (e.g. Article 58(1) c, e & f) (e.g. 58(2) a, b, c, d, e & g GDPR). If SAs are considered as exercising 'public powers' as understood under EU law, there is a possibility that SAs could be considered as acting like 'private persons' in 'civil and commercial matters' (e.g. in the field of international jurisdiction and applicable law).

In theory, SAs may exercise their investigative and corrective powers in a manner that produces effects beyond the EEA territories within the framework of the relevant international law. However, that does not necessarily imply that:

- third countries will accept that SAs exercise investigative and corrective powers in a manner that produces effects on their territories;
- third countries will accept that SAs initiate legal actions or proceedings before their courts or tribunals;
- third countries will recognise that SAs are acting in 'civil or commercial matters' or that they are exercising 'public powers';
- the rules applied by SAs in exercising their investigative and corrective powers are 'acceptable' or 'applicable' in the third countries' courts or tribunals;

- SAs are allowed to send agents abroad to third countries, even with the consent of the controllers/processors established in those countries.

Enforcement of EU SAs' decisions in courts in California and the UK may prove difficult - if not impossible - in a reasonable timeframe without prejudice to its financial cost. However, the adoption of the California Consumer Privacy Act of 2018 may open the door to active cooperation with the California Privacy Protection Agency. Similarly, cooperation with the UK Data Protection Commissioner seems possible in the context of Treaty 108+ (Articles 16 and 17), combined with the functions and missions vested in the UK Commissioner by the UK GDPR and Data Protection Act (DPA 2018). It is worth noticing that the UK Commissioner has concluded a relatively high number of Memorandum of Understanding (MoUs) with foreign data protection authorities. Cooperation with China seems possible in theory but would require a comprehensive approach, including close cooperation with the EU and the Member State public authorities responsible for that relationship with China.

3. Identification of legal instruments supporting the enforcement of SAs' powers

SAs identified legal instruments that could support the enforcement of the GDPR against third-country controllers and processors. The Study highlights some additional instruments that could usefully be considered.

4. Sharing SA experiences and identification of other types of actions

SAs have gained some informal experience of international cooperation. They have identified some avenues to improve international cooperation in the field of data protection, with direct action on the electronic communications infrastructure, or the intermediaries located on the EEA territories appearing most effective (e.g. order to stop collecting personal data or order to shut down a website).

5. Analysis of the possibility to rely on unilateral commitments from controllers/processors on the matters of choice of jurisdiction and applicable law

It appears quite difficult to rely on unilateral commitments from controllers and processors in respect of the choice of jurisdiction or applicable law. However, if SAs are considered to act in 'civil and commercial matters', that opens the way for discussions on the possibility of some degree of choice of jurisdiction and applicable law.

6. Analysis of added value of the designation of controller/processors representatives in the enforcement of SAs' investigative and corrective powers

The appointment of a controller/processor representative is a crucial point for the enforcement of SA investigative and corrective powers.

7. Main obstacles to international cooperation in the field of data protection

SAs have identified several obstacles to international cooperation in the field of data protection, such as lack of practice, shortcomings in the legal framework, problems in producing evidence.

In conclusion, strengthening international cooperation seems to be the best avenue for better and easier enforcement of SAs' investigative and corrective powers against third-country controllers or processors that fall under the scope of Article 3(2) of the GDPR but who are not willing to cooperate with SAs and did not designate an EEA representative. In the short term, the conclusion of MoU (or equivalent) should be considered. The use of legal instruments in the matter of criminal cooperation (such as the Mutual Legal Assistance Treaty (MLAT) concluded with the US) could be considered where there is a serious breach of the GDPR that amounts to a criminal offence. Finally, closer cooperation with the European

Commission when negotiating trade agreements could be useful in considering effective mechanisms to enforce SA investigative and corrective powers abroad.

1 INTRODUCTION

This is the Final Report for the study on ‘The enforcement of GDPR obligations against entities established outside the EEA but falling under Article 3(2) GDPR’ (the Study), prepared by CRIDS with the support of Milieu, under Specific Contract No Specific Contract No. 2020-1103 (EDPS/2019/02-09) for the European Data Protection Board (EDPB).

1.1 RESEARCH QUESTIONS AND SCOPE OF THE STUDY

Article 3(2) of the GDPR provides that:

'This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

- (a) *the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or*
- (b) *the monitoring of their behaviour as far as their behaviour takes place within the Union.'*

The Study analyses the practical and effective possibilities available to enforce Supervisory Authorities’ (SAs) investigative and corrective powers (as set out in Article 58(1) and (2) of the GDPR¹) against third-country controllers or processors that fall under the scope of Article 3(2) of the GDPR, but are not willing to cooperate with SAs and did not designate a European Economic Area (EEA) Representative.

The Study is limited to controllers and processors located in the State of California (United States of America, US) and in the United Kingdom of Great Britain and Northern Ireland (UK). Where possible, the study provides information on the situation in the People’s Republic of China (China). The Study is not limited to the analysis of the GDPR enforcement from the perspective of the five EEA countries mentioned in the Terms of Reference (ToR) (France, Germany, Poland, Spain and Sweden), but, rather, considers inputs received from all the SAs that responded to the questionnaire.

In the context of the Study, a first distinction should be made between:

- the possibility to summon controllers/processors to appear before the SA’s Office or in a Court in the SA’s country;
- the possibility for the SAs to enforce their investigative and corrective powers against controllers/processors.

The Study does not consider the broader discussion of the possibility for European legislation to produce extra-territorial effects, nor does it contain a theoretical analysis of the issues at stake. That means that the Study left open the numerous and difficult theoretical discussions which can be associated with its subject matter. This analysis is prepared without prejudice to the impact of the circumstances of each real case related to the enforcement of GDPR obligations against entities established outside the EEA.

1.2 METHODOLOGY

Two research methods were used in the Study:

- **Desk work:** desk research, entailing the thorough revision of legislation, international instruments, literature and case-law was completed prior to drafting a questionnaire for the

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, pp. 1–88.

SAs. The findings of the desk research were also used to structure the main project deliverables and guide the analysis provided in this Final Report. The desk research also entailed the revision of information received from the EDPB, the European Data Protection Supervisor (EDPS) and the European Commission in respect of national mechanisms and international agreements/treaties/mechanisms on the matter of enforcing the GDPR outside the EEA (including provisions that could exist in international trade agreements/treaties);

- **Questionnaire to SAs:** based on the desk research, a questionnaire was designed to collect information from all SAs on the enforcement of the GDPR obligations against entities established outside the EEA but falling under Article 3(2) of the GDPR (identification of specific legal mechanisms and issues, etc.). Sixteen SAs responded (BG, HR, CZ, DK, EE, FI, FR, HU, IS, IT, LT, LU, PL, SK, SI, SE). However, the Study would have benefitted from receiving answers from more SAs.

The Study comprised a series of logical methodological steps, as outlined in Box 1.

Box 1: Methodological steps in completing the Study

- | | |
|--|---|
| (1) Questionnaire: | <ul style="list-style-type: none">■ Drafting the questionnaire■ Validation of the questionnaire by the EDPB/EDPS■ Dissemination of the questionnaire to national SAs■ Completion of the questionnaire by national SAs |
| (2) Desk research: | <ul style="list-style-type: none">■ Compilation and analysis of the outcomes of the questionnaire■ Legal characterisation of the powers conferred on SAs by Article 58 GDPR■ Analysis of international instruments that could impact GDPR enforcement■ Analysis of binding corporate rules (BCR) and standard contractual clauses that could impact GDPR enforcement■ Analysis of the interaction between international public law and GDPR enforcement■ Analysis of the function of a representative (Article 27) and its relationship to GDPR enforcement■ Analysis of international cooperation (Article 50) |
| (3) Report drafting: | <ul style="list-style-type: none">■ Legal analysis and first draft of the Report■ Final version of the Report |
| (4) Quality assurance, editing and validation: | <ul style="list-style-type: none">■ Quality assurance by senior reviewer and editing■ Interim Meeting with the Client |
| (5) Finalisation: | <ul style="list-style-type: none">■ Delivery of the Final Report Draft■ Commenting period for client■ Addressing comments and finalising report■ Final meeting■ Delivery of the Final Report |

1.3 REPORT OUTLINE

This report is structured in three sections. Section 1 presents the background, scope and methodology, Section 2 analyses the various aspects of enforcing SAs' investigative and corrective powers, and Section 3 describes the main conclusions of the Study.

Annex 1 contains the template questionnaire used to collect information at EU and national level, Annex 2 lists the sources referenced in the Study, and Annex 3 presents the acronyms and abbreviations used.

2 LEGAL ANALYSIS

Section 2 provides a legal analysis of the following aspects:

- Possibility to summon third-country controllers/processors established in California or in the UK before SAs' Office or in a Court of the SA's country (Section 2.1);
- Analysis of the enforcement of SAs' investigative and correctives powers in California, the UK, and China (Section 2.2);
- Identification of the legal instruments that could support the enforcement of the GDPR against controllers/processors established in a third country (Section 2.3);
- Sharing SAs' experiences and identifying other types of actions (Section 2.4);
- Analysis of the possibility to rely on unilateral commitment from controllers/processors established outside the EEA on matters of choice of jurisdiction and applicable law (Section 2.5);
- Analysis of added value of controller/processor representatives in respect of enforcement of SA investigative and corrective powers (Section 2.6);
- International cooperation foreseen in the GDPR (Section 2.7).

2.1 POSSIBILITY TO SUMMON A THIRD-COUNTRY CONTROLLER/PROCESSOR

Section 2.1.1 outlines whether or not SAs have the legal possibility to summon third-country controllers/processors, as per their questionnaire responses.

Section 2.1.2, analyses whether or not third-country controllers/processors falling under the scope of Article 3(2) of the GDPR could be summoned in cases where they are not willing to cooperate with SAs and did not designate an EEA representative to appear before the SA's Office or in a Court of the SA's country.

Section 2.1.3 outlines a possible outstanding issue even were the right of SAs to summon third-country controllers/processors established in California and the UK to be solved.

2.1.1 Summary of SA responses

The SAs responses showed some uncertainties about the scope of the issue. Some specified possibilities of summoning a controller to appear before a court, others focused on summoning to the SA itself in the course of its administrative proceeding, and still others referenced reporting crimes to the public prosecutor. The same is true of bringing infringements to the attention of the judicial authorities, which may be understood as initiating a civil proceeding in order to defend data subjects' subjective personal rights (e.g. by a judicial order addressed to the controller to refrain from intervening into data subjects' rights to privacy and personality) or reporting crimes to criminal authorities (judicial included). Both understandings have different legal purposes and lead to different answers.

In Bulgaria, the SA has the legal possibility to summon a controller/processor to appear before a court (Article 10 a(2) point 1 of the Bulgarian Personal Data Protection Act (PDPA)). Only Bulgarian law will be applied.

In Czechia, if a person is summoned and fails to appear before an administrative authority without providing an appropriate explanation, the authority can impose a procedural fine of up to CZK 50,000 (EUR 1,956 EUR). A fine may be imposed more than once (Section 62(1,3) of the Administrative Procedure Code). The power to bring infringements of the GDPR to the attention of judicial authorities or to commence or otherwise engage in legal proceedings has not been implemented, however.

In Finland, the national legislation does not include specific data protection rules on the possibility to

summon a controller/processor to appear before a court. According to the Data Protection Act (1050/2018) Section 22 (Conditional fine):

'The Data Protection Ombudsman may impose a conditional fine for the purpose of enforcing an order referred to in points (c)–(g) and (j) of Article 58(2) of the Data Protection Regulation and to enforce an order to provide information that has been issued under section 18, subsection 1 of this Act. Provisions on the imposition of a conditional fine and the ordering of its payment are laid down in the Act on Conditional Fines (1113/1990).

No conditional fine shall be imposed on a natural person for the purpose of enforcing an order to provide information referred to in subsection 1 if there are grounds to suspect the person of a criminal offence and the information concerns the matter underlying the suspicion of a criminal offence.'

However, the Finnish SA has yet to apply Section 22 in practice.

In France, the SA (*Commission nationale de l'informatique et des libertés*, CNIL) has the power to sanction a data controller falling under the scope of Article 3(2) of the GDPR. In that case, the CNIL will pronounce an administrative sanction. The difficulty here lies in enforcement of this decision abroad. A solution is to transfer breaches to the Criminal Court, whose decisions can be enforced in third countries, and GDPR breaches are, in fact, also criminal offences under French law. The French courts will apply the French data protection law. Processing is not qualified as ‘cross-border processing’ if the data controller has no establishment within the EU, even if personal data of data subjects in the Union are processed by that data controller. The GDPR applies but is not cross-border processing subject to mandatory cooperation between European SAs.

In Croatia, Article 38 of the Act on the Implementation of the General Data Protection Regulation sets out that if, during supervision, knowledge is gained or objects are found that indicate a criminal offence has been committed that could be prosecuted *ex officio*, the authorised persons shall, within the shortest time possible, inform the competent police station or a state attorney. It is unclear whether the SA may summon a controller/processor before the court or to its Office.

In Hungary, Section 2 (5) b) of the Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (DPA Act) prescribes the following:

'Where personal data are processed within the meaning of the General Data Protection Regulation, the provisions of this Act specified in Subsection (2), and other regulations provided for by law laying down conditions for the protection of personal data and for the processing of personal data shall apply - save where an act or binding legislation of the European Union provides otherwise - if:

(...)

b) the main establishment provided for in Point 16 of Article 4 of the General Data Protection Regulation of the data controller, or the single establishment of the data controller in the European Union is not located in Hungary, however, the processing operations carried out by the controller or processor acting on the controller's behalf or following the controller's instructions, are related to ba) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in Hungary, or bb) the monitoring of the data subjects' behaviour as far as their behaviour takes place within the territory of Hungary.'

In Iceland, the SA does not have the power to summon a processor/controller to appear before the SA’s Office or a court.

In Italy, the Italian SA has the power to summon a processor/controller to appear before the SA’s Office or a court (for the latter, see: Article 154-b of the Italian Data Protection Code). The Italian SA considers

that Articles 77, 78 and 79 of the GDPR are the legal bases for the application of the GDPR, also *vis-à-vis* an Article 3(2) controller/processor. The laws will be the same as those applied to a controller/processor under Article 3(1) of the GDPR. Apart from the GDPR rules, Section 166, paragraph 7, of the Data Protection Code, Law No 689/1981 relating to the application of administrative fines (in particular Sections 1-9, 18-22, 24-28) should be applied. Where necessary, Law No 241/1990 on Administrative Procedure and the Right of Access to Administrative Documents and the relevant Italian Freedom of Information Act provisions (Section 5 and 5-a of Legislative Decree No 33 of 2013) could also be applied.

In Lithuania, pursuant to Article 12(2)(9) of the Republic of Lithuania Law on Legal Protection of Personal Data ('the Law'), the SA has the right to receive oral and written explanations from legal and natural persons during the investigation of violations and to demand that they come to the premises of the State Data Protection Inspectorate (SDPI) to give explanations. Pursuant to Article 12(2)(7) of the Law, the SDPI has the right to take part in court proceedings in cases of violations of international, EU and national law provisions on the protection of personal data.

In Luxembourg, no specific procedure is foreseen in national law to allow the SA to directly sue a controller/processor before the courts in relation to Article 58(5) GDPR.

In Poland, in cases of claims for infringements of data protection provisions that can only be asserted in court proceedings, the President of the Polish SA may bring actions in favour of the data subject, with their consent (Article 98(1) of the Act of 10 May 2018 on Personal Data Protection). In such cases, the Act of 17 November 1964, Code of Civil Procedure (Journal of Laws of 2020, item 1575, 1578 and 2320; Journal of Laws of 2021, item 11) is applied.

In Slovenia, the SA does not have the power to summon a processor/controller to appear before the SA's Office or a court.

2.1.2 Consequences of Case C-645/19 on the interpretation of Article 58(5) of the GDPR

In case C-645/19² (§§ 78-79), the CJEU ruled that the exercise of Article 58(5) of the GDPR by an SA is not subject to the condition that the controller/processor be established on the territory of the SA's Member State:

'It must be observed that Article 58(5) of Regulation 2016/679 is worded in general terms and that the EU legislature has not specified that the exercise of that power by a Member State's supervisory authority is subject to the condition that its legal action should be brought against a controller who has a "main establishment", within the meaning of Article 4, point 16, of that regulation, or another establishment on the territory of that Member State'.

In addition to this point, the CJEU has limited the consequence of its previous consideration to the condition that the SA's power falls within the territorial scope of the GDPR (with reference to Article 3(1), but also to Article 3(2) and (3) of the GDPR) (Id., §§ 80-84):

'80. However, a Member State's supervisory authority may exercise the power conferred on it by Article 58(5) of Regulation 2016/679 only if it is demonstrated that that power falls within the territorial scope of that regulation.

'81. Article 3(1) of Regulation 2016/679, which governs the territorial scope of that regulation, provides, in that regard, that the regulation applies to the processing of personal

² Case C-645/19: Request for a preliminary ruling from the *Hof van beroep te Brussel* (Belgium) lodged on 30 August 2019 — Facebook Ireland Limited, Facebook Inc., Facebook Belgium BVBA v *Gegevensbeschermingsautoriteit*, OJ C 406, 2.12.2019.

data in the context of the activities of an establishment of a controller or a processor in the European Union, whether or not the processing takes place in the European Union.

82. *In that connection, recital 22 of Regulation 2016/679 states that the existence of such an establishment implies the effective and real exercise of activity through stable arrangements and that the legal form of such arrangements, whether through a branch or a subsidiary with legal personality, is not the determining factor in that respect.*

83. *It follows that, in accordance with Article 3(1) of Regulation 2016/679, the territorial scope of that regulation is determined, without prejudice to the situations referred to in paragraphs 2 and 3 of that article, by the condition that the controller or the processor with respect to the cross-border processing has an establishment in the European Union.*

84. *Consequently the answer to the second question referred is that Article 58(5) of Regulation 2016/679 must be interpreted as meaning that, in the event of cross-border data processing, it is not a prerequisite for the exercise of the power of a supervisory authority of a Member State, other than the lead supervisory authority, to initiate or engage in legal proceedings, within the meaning of that provision, that the controller with respect to the cross-border processing of personal data against whom such proceedings are brought has a main establishment or another establishment on the territory of that Member State.'*

The CJEU also stressed the link between Article 58(5) of the GDPR and the exercise of SAs' powers on their national territory, irrespective of the Member State in which the controller/processor is established (Id., §§ 88-91 & 96):

'88. *As regards the power of a supervisory authority of a Member State to bring legal proceedings, within the meaning of Article 58(5) of Regulation 2016/679, it must be recalled, as the Advocate General stated in point 150 of his Opinion, that that provision is worded in general terms and that it does not specify against which entities the supervisory authorities should or might direct legal proceedings in relation to any infringement of that regulation.*

89. *Consequently, that provision does not restrict the exercise of the power to initiate or engage in legal proceedings in such a way that those proceedings can solely be brought against a "main establishment" or against some other "establishment" of the controller. On the contrary, under Article 58(5) of that regulation, where the supervisory authority of a Member State has the necessary competence for that purpose, under Articles 55 and 56 of Regulation 2016/679, it may exercise the powers conferred by that regulation on its national territory, irrespective of the Member State in which the controller or its processor is established.*

90. *However, the exercise of the power conferred on each supervisory authority in Article 58(5) of Regulation 2016/679 presupposes that that regulation is applicable. In that regard, and as stated in paragraph 81 of the present judgment, Article 3(1) of that regulation provides that it is applicable to the processing of personal data 'in the context of the activities of an establishment of a controller or a processor in the [European] Union, whether or not the processing takes place in the [European] Union'.*

91. *Having regard to the objective pursued by Regulation 2016/679, which is to ensure effective protection of the freedoms and fundamental rights of individuals, in particular, their right to protection of privacy and the protection of personal data, the condition that the processing of personal data must be carried out "in the context of the activities" of the establishment concerned, cannot be interpreted restrictively (see, by analogy, judgment of 5 June 2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388, paragraph 56 and the case-law cited).*

96. (...) the power of a supervisory authority of a Member State, other than the lead supervisory authority, to bring any alleged infringement of that regulation to the attention of a court of that Member State and, where appropriate, to initiate or engage in legal proceedings, within the meaning of that provision, may be exercised both with respect to the main establishment of the controller which is located in that authority's own Member State and with respect to another establishment of that controller, provided that the object of the legal proceedings is a processing of data carried out in the context of the activities of that establishment and that that authority is competent to exercise that power, in accordance with the terms of the answer to the first question referred.'

The CJEU confirmed that Article 58(5) of the GDPR has direct effect, '*(...) with the result that a national supervisory authority may rely on that provision in order to bring or continue a legal action against private parties, even where that provision has not been specifically implemented in the legislation of the Member State concerned (...)*' (Id., §§ 111 & 113):

'(...) Article 58(5) of Regulation 2016/679 lays down a specific and directly applicable rule which states that the supervisory authorities must have legal standing before the national courts and must have the power to initiate or engage in legal proceedings under national law.'

The Court added that there was no need for specific implementation in national law (Id., §§ 111 & 113):

'(...) Article 58(5) of Regulation 2016/679 must be interpreted as meaning that that provision has direct effect, with the result that a national supervisory authority may rely on that provision in order to bring or continue a legal action against private parties, even where that provision has not been specifically implemented in the legislation of the Member State concerned.'

Those questions being settled, it remains to understand whether this judgment could be relied on in assessing whether Article 58(5) GDPR may also be used by SAs against a third-country controller/processor that falls under the scope of Article 3(2) GDPR but is not willing to cooperate with SAs and did not designate an EEA representative to appear in a court in their Member States.

The CJEU appeared to consider Article 58(5) of the GDPR available to SAs as soon as the GDPR applies to the controller, i.e. when the processing of personal data falls under the territorial scope of the GDPR (Article 3), including its application in the situations considered in Article 3(2)-(3).

However, the CJEU also seemed to hold that SAs must exercise their powers on their national territory. It is not clear whether this precludes SAs from initiating legal proceedings in another Member State or in a third country on the basis of Article 58(5) of the GDPR.

The position of the CJEU in respect of the possibility to open any 'international jurisdiction or competence' to the benefit of any 'court or tribunal' of the Member State of the SA on basis of Article 58(5) of the GDPR in cases where the controller/processor lacks any kind of establishment on the territory of any of the Member States, is also unclear.

One possible interpretation is that SAs should be recognised as having the power to summon a third-country controller/processor that falls under the scope of Article 3(2) of the GDPR but is not willing to cooperate with SAs and did not designate an EEA representative to appear in court in their Member State, based on Article 58(5) of the GDPR, for at least four reasons:

- Controller/processor is subject to the GDPR in its totality. There is no formal reason to exclude Article 58(5) of the GDPR;
- As judged by the CJEU, 'the condition that the processing of personal data must be carried out "in the context of the activities" of the establishment concerned, cannot be interpreted restrictively';

- There might be no possibility to initiate any legal proceeding against the controller/processor in the country where it is located or established (for reasons relating to the interpretation of Article 58(5) of the GDPR by the CJEU, or for reasons stemming from the third country's legal rules);
- It could lead to an unexpected competitive distortion between EU-based and non-EU-based controllers/processors.

On the other hand, it should not be disputed that SAs are entitled to summon a third-country controller/processor that falls under the scope of Article 3(2) of the GDPR, but is not willing to cooperate with SAs and did not designate an EEA representative to appear before its Office, based on the provisions of their national law implementing the GDPR.

2.1.3 Key findings

There are differences between SAs' powers to summon third-country controllers/processors to appear before the SA's Office or in a Court of the SA's country. There are uncertainties as to the possibility for SAs to initiate legal proceedings in another EU Member States or in a third country on the basis of Article 58(5) of the GDPR. The CJEU case-law is unclear as to whether it could accept to recognise the jurisdiction of a Member State on the basis of Article 58(5) of the GDPR when the controller/processor has no establishment on the territory of any EU Member State.

If the option to summon a controller/processor that falls under the scope of Article 3(2) of the GDPR but is not willing to cooperate with SAs and did not designate an EEA representative before the SA's Office or a court is initiated, the question of the enforcement of the decision remains, where that controller/processor is uncooperative or does not comply with the court's decision or order.

2.2 ANALYSIS OF ENFORCEMENT OF SAs' INVESTIGATIVE AND CORRECTIVE POWERS IN CALIFORNIA, THE UK AND CHINA

Section 2.2.1 provides a brief analysis of the nature of SAs' investigative and corrective powers.

Section 2.2.2 outlines the possibility for SAs to exercise their investigative and corrective powers beyond the EEA territories.

Section 2.2.3 describes SAs' investigative and corrective powers in California against third-country controllers or processors that fall under the scope of Article 3(2) of the GDPR but are unwilling to cooperate with SAs and did not designate an EEA representative.

Section 2.2.4 outlines SAs' investigative and corrective powers in the UK against third-country controllers or processors that fall under the scope of Article 3(2) of the GDPR but are unwilling to cooperate with SAs and did not designate an EEA representative.

Section 2.2.5 describes SAs' investigative and corrective powers in China against third-country controllers or processors that fall under the scope of Article 3(2) of the GDPR but are unwilling to cooperate with SAs and did not designate an EEA representative.

2.2.1 First preliminary remark: The nature of SAs' investigative and corrective powers

When considering the enforcement of the SAs' investigative and corrective powers against a third-country controller/processor established in California, the UK or China, that falls under the scope of Article 3(2) of the GDPR but is not willing to cooperate with SAs and did not designate an EEA representative, the first issue to analyse is the nature of the SAs' powers.

First, we could think that the nature of SAs' powers should be assessed under the national legislation of the SA's Member State. However, this approach would overlook the fact that SAs now have their legal

basis, status and regime under the GDPR, which is a piece of European legislation (cf. C-645/19, §44).

The issue of determining the nature of the SAs' investigative and corrective powers should therefore be analysed under EU law, with national law characteristics examined only where prescribed or authorised by the GDPR (e.g. Article 58(1)f of the GDPR) or when it is compatible with the GDPR and EU law (including CJEU case-law of the CJEU).

An analysis of all aspects of this (very broad) topic would go beyond the scope of this Study and require far more elaboration (e.g. do SAs qualify as 'European administrative' 'bodies' or 'agencies' or as 'European administrative authorities'). Rather, the Study focuses on two specific aspects that are of interest in the analysis of the nature of SAs' investigative and corrective powers:

- Could SAs qualify as 'courts or tribunals' in the meaning of Article 267 TFEU³ when exercising their investigative and corrective powers?
- Could SAs be considered to exercise 'public powers' when exercising their investigative and corrective powers?

2.2.1.1 The notion of 'court or tribunal' in the meaning of Article 267 of the TFEU

According to the case-law of the CJEU (e.g. Case VQ v Land Hessen⁴, §43), in order to determine whether a body is a 'court or tribunal' within the meaning of Article 267 of the TFEU, the CJEU considers several factors, such as whether:

- the body is established by law;
- the body is permanent;
- the body's jurisdiction is compulsory;
- the body's procedure is *inter partes*;
- the body applies rules of law;
- whether the body is independent.

In this Study it is argued that there is no dispute over the fact that SAs do not qualify as 'courts or tribunals' in the meaning of Article 267 of the TFEU while exercising their investigative and corrective powers. This derives from the interpretation of Article 78 of the GDPR, for example, which provides each natural or legal person with the right to an effective judicial remedy against a legally binding decision of an SA concerning them. If SAs were to be qualified as 'courts or tribunal', this provision would lack meaning⁵.

2.2.1.2 The notion of the exercise of 'public powers' in CJEU case-law

While it could easily be concluded that SAs do not qualify as 'courts or tribunals' in the meaning of Article 267 of the TFEU while exercising their investigative and corrective powers, it is less straightforward to assess whether in doing so they exercise 'public powers'.

The case-law of the CJEU (notably in the field of consumer law) may provide some elements to determine whether SAs are exercising 'public powers' (e.g. *Case Belgische Staat v Movic BV, Events Belgium BV, Leisure Tickets & Activities International BV*⁶). The main elements to consider are:

³ Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012, pp. 47–390.

⁴ Judgment of the Court (Third Chamber) of 9 July 2020, VQ v Land Hessen VQ v Land Hessen.

⁵ See: EDPS, *Data protection in the judiciary: the concept of courts/judicial authorities acting in their judicial capacities*, EDPS/2019/02-01, July 2020.

⁶ CJEU, 16 July 2020, *Belgische Staat v Movic BV, Events Belgium BV, Leisure Tickets & Activities International BV*, C-73/19.

'In order to ensure, as far as possible, that the rights and obligations which derive from Regulation No 1215/2012 for the Member States and the persons to whom it applies are equal and uniform, the concept of "civil and commercial matters" of that regulation should not be interpreted as a mere reference to the internal law of a Member State. That concept must be regarded as an autonomous concept to be interpreted by reference, first, to the objectives and scheme of that regulation and, second, to the general principles which stem from the corpus of the national legal systems (Id., §33).'

'Although certain actions where the opposing parties are a public authority and a person governed by private law may come within the scope of Regulation No 1215/2012, it is otherwise where the public authority is acting in the exercise of its public powers (Id., §35).'

'The exercise of public powers by one of the parties to the action, because it exercises powers falling outside the scope of the ordinary legal rules applicable to relationships between private individuals, excludes such an action from "civil and commercial matters" within the meaning of Regulation No 1215/2012 (Id., §36).'

'It follows that, in order to determine whether or not a matter falls within the scope of the concept of "civil and commercial matters" within the meaning of Regulation No 1215/2012, and, consequently, whether it comes within the scope of that regulation, it is necessary to determine (Id., §37):

- *the nature of the legal relationships between the parties to the action and the subject matter of the action;*
- *or, alternatively, the basis of the action and the detailed rules applicable to it.'*

'Actions aimed at determining and stopping unfair commercial practices, within the meaning of Directive 2005/29, are also "civil and commercial matters" within the meaning of Article 1(l) of Regulation No 1215/2012 (Id., §42).'

'The fact that a power was introduced by legislation is not, in itself, decisive in order to conclude that a State authority acted in the exercise of public powers (Id., §47).'

'It follows that the procedural position of the Belgian authorities is, in that regard, comparable to that of a consumer protection association (Id., §49).'

'Acting in the general interest should not be confused with the exercise of public powers (Id., §53).'

'Only where, due to the use to which a public authority has put certain pieces of evidence, it is not specifically in the same position as a person governed by private law in the context of a similar action, would it be appropriate to make a finding that such an authority has, in the particular case, exercised public powers (Id., §57).'

'It should be pointed out that merely collecting and compiling complaints or evidence, as a trade or consumer association could do, cannot amount to the exercise of such powers (Id., §58).'

'However, as regards the application made by the Belgian authorities to the referring court that it should be granted the power to determine future infringements simply by means of a report issued, on oath, by an official of the Directorate-General for Economic Inspection, such an application cannot be said to come within the scope of 'civil and commercial matters', as that application relates in actual fact to special powers that go beyond those arising from the ordinary legal rules applicable to relationships between private individuals (Id., §62).'

Deriving from the above, it is understood that SAs could be considered to exercise ‘public powers’ under EU law when making use of special powers that go beyond those arising from the ordinary legal rules applicable to relationships between private individuals, such as the power to:

- oblige controllers/processors to appear before their Offices;
- inflict fines;
- issue enforceable orders;
- exercise coercive means or methods;
- impose coercive measures;
- act in the capacity of judicial officer;
- draw up authentic statement or report (‘on oath’), etc.

It could also be necessary to consider:

- the nature of the legal relationships between the parties to the action and the subject matter of the action; or
- the basis of the action and the detailed rules applicable to it.

It seems certain that the mere existence of investigative powers conferred by law is not enough to characterise the exercise of ‘public powers’. In other words, SAs must exercise some kind of ‘coercive powers’⁷ without prejudice to considering (to some extent) the characteristics of the specific powers that might have been conferred upon them by their national law.

With respect to the exercise of ‘public powers’ as understood in the CJEU case-law, the wording of Article 58 of the GDPR might be slightly misleading in respect of the nature of some investigative powers (e.g. Article 58(1)c, e, f of the GDPR) and even some corrective powers (e.g. Article 58(2)a, b, c, d, e, g of the GDPR). As a consequence, the very nature of these powers should have to be additionally ascertained in light of the powers conferred on SAs by their national data protection laws: do the latter provide SAs with exorbitant powers that are distinct from those recognised to data subjects or not-for-profit bodies, organisations or associations referred to in Article 80(1) of the GDPR? This will have to be analysed on a case-by-case basis.

2.2.2 Second preliminary remark: The possibility to exercise SAs’ investigative and corrective powers beyond the EEA territories

As Freyria already wrote in the 1960s about the potential extra-territorial effects of public law:

‘It is traditional to assert that public law is territorial. The proposal is flawed by its absolutism and imprecision. Despite its territoriality, social security law follows nationals abroad. A French person who has suffered an accident at work will benefit from the pensions despite his departure abroad. He will receive his old-age insurance pension there as long as he has paid his contributions within the regulatory time limits. In the same way, our tax law imposes a general tax on the French source income received by the French person who leaves to reside abroad. (...) In all these cases, there is no coincidence of our legislation with the geographical framework of our territory. Research must continue well beyond such a primary and superficial formula. (...)’⁸.

In 2018, Azzi recalled that investigation cannot be perform on a foreign territory:

⁷ Idot, L., ‘La matière civile et commerciale’ à l’épreuve de l’intervention du Ministre de l’Economie en droit de la consommation, note sous CJUE (1e ch.), 16 Juillet 2020, aff. C-73/19, *Revue critique de droit international privé*, Paris, Dalloz, 2021/2, p. 383 & s., esp. p. 394, n° 15.

⁸ Freyria, Ch., ‘La notion de conflit de lois en droit public’, in *Travaux du Comité français de droit international privé*, 1962-1964, pp. 106-107.

*'Under international law, it is prohibited for a state to perform an act on foreign territory when it falls within the exclusive competence of the foreign state officials, such as investigation. The consent of the foreign state must be obtained, regardless of the consent of the parties. This rule is shared by every country, including China which codified it under Article 277 of CiPL'*⁹.

She added that:

*'Some authors mention the possibility of resorting to international cooperation agreement, such as agreement of mutual legal assistance (MLA). Currently, the vast majority of those treaties are related to criminal cases'*¹⁰.

*'Regarding data protection, some punctual authorisations have been given. It happened for the first time in 1996, when the German DPA obtained the consent of Citibank to conduct an on-site audit of the data processing facilities of its US subsidiary, which had received the credit card data of German customers. A further example is given by the Spanish DPA, which also conducted an audit on the processing equipment of a data recipient in Colombia, on the basis of a contractual clause authorising such an investigation'*¹¹.

*'These cases raise the question as to whether the cooperation could actually be organised through contractual clauses. Actually, some standard contractual clauses for data transfers outside the EU already contain a prior authorisation given to the relevant DPA. However, as noted by Christopher Kuner, the consent of the relevant government authorities will always be required and, according to him, was obtained by the German and Spanish DPAs in the cases mentioned'*¹².

*'An EU DPA may also overcome the reluctance to consent of the foreign authorities by asking its DPA to conduct the measures itself, on behalf of the EU DPA, but an agreement would have to be reached as to the costs incurred by the operation'*¹³.

On the one hand, in case C-18/18, the CJEU judged that Directive 2000/31/EU¹⁴ does not preclude national courts from issuing orders that could produce effects beyond the EEA territories, but within the framework of the relevant international law¹⁵:

'Directive 2000/31, in particular Article 15(1), must be interpreted as meaning that it does not preclude a court of a Member State from:

- *ordering a host provider to remove information which it stores, the content of which is identical to the content of information which was previously declared to be unlawful, or to block access to that information, irrespective of who requested the storage of that information;*
- *ordering a host provider to remove information which it stores, the content of which is equivalent to the content of information which was previously declared to be unlawful, or to block access to that information, provided that the monitoring of and search for the information concerned by such an injunction are limited to information conveying a message the content of which remains essentially unchanged compared with the content which gave rise to the finding of illegality and containing the elements specified in the*

⁹ Azzi, A., 'The challenges faced by the extraterritorial scope of the General Data Protection Regulation', *Journal of Intellectual Property, Information Technology and e-Commerce Law*, Vol. 9, No. 2, 2018, p. 59.

¹⁰ Ibid., p. 60.

¹¹ Ibid., p. 61.

¹² Ibid., p. 62.

¹³ Ibid., p. 63.

¹⁴ 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').

¹⁵ CJEU, 3 October 2019, Eva Glawischnig-Piesczek v Facebook Ireland Limited, C-18/18, §53.

- injunction, and provided that the differences in the wording of that equivalent content, compared with the wording characterising the information which was previously declared to be illegal, are not such as to require the host provider to carry out an independent assessment of that content, or*
- *ordering a host provider to remove information covered by the injunction or to block access to that information worldwide within the framework of the relevant international law.'*

Therefore, *mutatis mutandis*, it does not seem impossible to consider that SAs may exercise their investigative (based on the argument *a maiore ad minus*) and corrective powers in a manner that produces effects beyond the EEA territories within the framework of the relevant international law.

However, third countries are bound by neither EU law nor CJEU case-law. It should be reiterated that in the absence of any international convention or treaty or any suitable national legal provision provided in third countries' own legislation, it does not necessarily follow from the interpretation of the CJEU's case-law in the field of eCommerce that:

- third countries will accept SAs exercising investigative and corrective powers in a manner that produces effects on their territories;
- third countries will accept SAs initiating legal actions or proceedings before their courts or tribunals;
- third countries will recognise that SAs are acting in 'civil or commercial matters' or that they are exercising 'public powers';
- the rules applied by SAs when exercising their investigative and corrective powers are 'acceptable' in the third countries' courts or tribunals¹⁶;
- SAs are allowed to send agents abroad to third countries, even with the consent of the controllers/processors established in those countries.

It results from these two preliminary remarks that SAs do not qualify as 'courts or tribunals' in the meaning of Article 267 of the TFEU while exercising their investigative and corrective powers, and they should be considered to exercise 'public powers' under European law only when making use of special powers that go beyond those arising from the ordinary legal rules applicable to relationships between private individuals. It also results from these two preliminary remarks that, in theory, SAs may exercise their investigative and corrective powers in a manner that produces effects beyond the EEA territories, albeit within the framework of the relevant international law.

2.2.3 The enforcement of SAs' investigative and corrective powers in California

It is assumed that European SAs are entitled - or have the power - to engage legal actions outside the EEA, in particular in the US (California), either on the basis of Article 58(5) of the GDPR or their national legislation. Notwithstanding, this subsection considers possible different legal instruments to support enforcement of SAs' investigative and corrective powers.

2.2.3.1 General findings on recognition and enforcement of foreign judgments and administrative acts in the US

(a) The lack of international conventions or treaties on the recognition and enforcement of foreign judgments

¹⁶ See e.g. *mutatis mutandis*: United States Court of Appeals, Yahoo! Inc. v. *La Ligue contre le racisme et l'antisémitisme et l'Union des étudiants juifs de France*, 433 F.3d 1199, 1202 (9th Cir. 2006) (en banc); M. Chivvis, 'Reexamining the Yahoo! litigations: toward an effects test for determining international cyberspace jurisdiction', *University of San Francisco Law Review*, Vol. 41, 2007, p. 699.

No international convention or treaty facilitates the recognition and enforcement of foreign judgments between the US and any other country¹⁷.

(b) The lack of a federal legislation on the recognition and enforcement of foreign judgments

The US *Congress has passed no law generally regulating the recognition and enforcement of foreign judgments*¹⁸. In addition, ‘*Foreign judgments are not constitutionally entitled to full faith and credit*¹⁹.

However, no rule prohibits the enforcement of foreign judgments. On the contrary, it seems to be considered that ‘*the Supreme Court in Hilton v. Guyot suggested long ago that considerations of international comity (recognition and deferral to foreign legislative, executive and judicial acts) may provide a basis for US foreign judgment enforcement*²⁰.

(c) Recognition and enforcement of foreign judgments is a matter for State law

Recognition and enforcement of foreign judgments are generally viewed as a matter for State law²¹ and are, in principle, ruled by State rather than federal law.

(d) Reciprocity requirement in the matter of recognition and enforcement of foreign judgments

Reciprocity no longer seems to be pivotal element in the recognition and enforcement of foreign judgments²².

(e) Uncertainty about the court or tribunal in which to bring suits for recognition and enforcement of foreign judgments

It is not always clear whether the suit should be brought before a federal court or a State court. However, even in a federal court, recognition and enforcement remain State law²³.

(f) Some general procedural requirements

The US court, State court or tribunal must have ‘subject matter jurisdiction over a case’, the case must be ‘justiciable’ and the US or State court or tribunal must have ‘personal jurisdiction’ over the defendant²⁴. The latter calls for the following observations:

‘*Personal jurisdiction refers to a court’s power over the parties in a proceeding. Personal jurisdiction means that a given court has power over a particular defendant. Traditionally, courts based jurisdiction upon territoriality or physical presence in the forum. (...)*²⁵.

Personal jurisdiction covers two notions: general jurisdiction and specific jurisdiction: ‘*General*

¹⁷ Folsom, R., *Principles of International Litigation and Arbitration*, 2d ed., West Academic, Concise Hornbook, 2019, pp. 447-490; Spillenger, Cl., *Principles of Conflict of Laws*, 3d ed., West Academic, Hornbook Series, 2020, pp. 453-454.

¹⁸ Ibid., pp. 453-454.

¹⁹ Ibid., p. 451.

²⁰ Folsom, R., *Principles of International Litigation and Arbitration*, 2d ed., West Academic, Concise Hornbook, 2019, pp. 447-490.

²¹ Ibid., pp. 447-490; Spillenger, Cl., *Principles of Conflict of Laws*, 3d ed., West Academic, Hornbook Series, 2020, p. 453; Bradley, C.A., *International Law in the U.S. Legal System*, 3d ed., Oxford University Press, 2021, pp. 10-11.

²² Spillenger, Cl., *Principles of Conflict of Laws*, 3d ed., West Academic, Hornbook Series, 2020, pp. 452-453, p 454; Bradley, C.A., *International Law in the U.S. Legal System*, 3d ed., Oxford University Press, 2021, pp. 10-11.

²³ Folsom, R., *Principles of International Litigation and Arbitration*, 2d ed., West Academic, Concise Hornbook, 2019, pp. 447-490.

²⁴ Bradley, C.A., *International Law in the U.S. Legal System*, 3d ed., Oxford University Press, 2021, pp. 2-8.

²⁵ Rustad, M., *Global Internet Law*, 3d ed., West Academic, Hornbook Series, 2020, pp. 182-183.

jurisdiction may be used to maintain a suit against a defendant even when it does not arise out of the defendant's activities in the forum state. In contrast, specific jurisdiction allows for a suit to be maintained only when the defendants' contacts with the forum are also the basis for the suit. (...)'²⁶.

*'General jurisdiction refers to the authority of a court to hear any cause of action involving a defendant, even those unrelated to the defendant's contacts with the forum State. For the court to have general jurisdiction over a corporation, there must be continuous and systematic contacts such as that a corporation is "essentially at home" in the forum state'*²⁷.

(g) Recognition and enforcement of foreign-country money judgments

When considering the enforcement of SAs' investigative and corrective powers (especially when they impose an administrative fine), consideration must be given to the implementation of the revised version of the 1962 Uniform Foreign-Country Money Judgments Recognition Act²⁸ (see below, on its implementation in California).

(h) Uncertainties about the scope of the recognition and enforcement of foreign judgments

US courts may recognise a foreign judgment or it may additionally enforce it (wholly or in part)²⁹, depending on the circumstances of each case.

(i) The law applicable to the suit for the recognition and enforcement of foreign judgments

In any case, there are no clear or settled rules regarding the question of the applicable law. However, it seems that *United States courts will not, however, apply the penal, revenue, or other public laws of foreign nations'*³⁰.

(j) Recognition and enforcement of administrative acts from foreign nations

The status and regime of administrative acts from foreign nations is unclear:

*'Administrative acts from foreign nations have generally not been treated as judgments except when their review, and the local forum's freedom to alter their result was precluded by supervening executive action or such notions as the "act of state" doctrine. The earlier proposal for a US-UK Recognition-of-Judgments Convention would have expressly limited its application to "judgments" of "courts". On the one hand, the Brussels-I (Recast) Regulation provides that it applies to "civil and commercial matters whatever the nature or tribunal," thereby including administrative tribunals of a judicial nature. Thus, while the recognition provisions (Art. 36 et seq.) only refer to "judgments," it may be true that "the distinction between judgments and administrative acts is generally losing ground together with its obsolescent rationale, and some cases bear this out'*³¹.

There is a possibility here for a US or State court or tribunal to recognise that an administrative act from a foreign nation could fall under the notion of 'civil or commercial matters' and be treated as a foreign judgment. To date, however, there is no other indication of the validity of this analysis in either the US

²⁶ Ibid., pp. 184-185.

²⁷ Rustad, M., *Global Internet Law*, 3d ed., West Academic, Hornbook Series, 2020, p. 187.

²⁸ Folsom, R., *Principles of International Litigation and Arbitration*, 2d ed., West Academic, Concise Hornbook, 2019, pp. 447-490.

²⁹ Ibid., pp. 447-490.

³⁰ Bradley, C.A., *International Law in the U.S. Legal System*, 3d ed., Oxford University Press, 2021, p. 14.

³¹ Hay, P., Borchers, P.J., Symeonides, S.C and Whytock, Chr. A., *Conflict of Laws*, 6th ed., West Academic, Hornbook Series, 2018, p. 1450.

legal doctrine or case-law.

(k) **Impact of the ‘Act of State Doctrine’**

The ‘Act of State Doctrine’ seems to allow for the recognition of the validity of foreign government acts³². Although not relevant for the Study, it is mentioned for the sake of completeness.

2.2.3.2 The 2003 Agreement on mutual legal assistance between the European Union and the United States of America

In 2001, the US and the Republic of Ireland concluded an Agreement relating to mutual legal assistance in criminal matters (Mutual Legal Assistance Treaty or MLAT). Two years later, in 2003, the US and the EU also concluded an Agreement relating to mutual legal assistance in **criminal matters** (the 2003 MLAT).

Article 5 of the 2003 MLAT allows for the constitution and operation of **joint investigative teams** ‘*for the purpose of facilitating criminal investigations or prosecutions involving one or more Member States and the United States of America where deemed appropriate by the Member State concerned and the United States of America*’³³.

The 2003 MLAT allows for the use of ‘**video conferencing** between each Member State and the United States of America for taking testimony in a proceeding for which mutual legal assistance is available of a witness or expert located in a requested State, to the extent such assistance is not currently available’³⁴.

It also provides for mutual legal **assistance** ‘*to a national administrative authority, investigating conduct with a view to a criminal prosecution of the conduct, or referral of the conduct to criminal investigation or prosecution authorities, pursuant to its specific administrative or regulatory authority to undertake such investigation. Mutual legal assistance may also be afforded to other administrative authorities under such circumstances. Assistance shall not be available for matters in which the administrative authority anticipates that no prosecution or referral, as applicable, will take place*³⁵.

While an EEA SA could try and use 2003 MLAT in cases where violation of a national data protection provision would result in a criminal penalty, it is clear that the 2003 MLAT is not designed to apply to all kinds of cases and its application is not unconditional. In fact, the US authorities do not seem to support the use of MLAT for minor criminal cases.

2.2.3.3 The “Undertaking Spam, Spyware, and Fraud Enforcement With Enforcers beyond Borders Act of 2006” (the ‘US Safe Web Act of 2006’)

Among other things, the US Safe Web Act of 2006 gives the US Federal Trade Commission (FTC) the authority to provide evidence to foreign law enforcement agencies to support appropriate foreign investigations or enforcement actions.

‘*A key requirement is that such proceedings address conduct substantially similar to something that would violate a law the FTC enforces*’³⁶.

The Act defines foreign law enforcement agencies as:

³² Bradley, C.A., *International Law in the U.S. Legal System*, 3d ed., Oxford University Press, 2021, pp. 11-14.

³³ Article 5(1) of the 2003 MLAT; Article 5(2) and (4) of the 2003 MLAT for the procedures under which the team is to operate.

³⁴ Article 6 of the 2003 MLAT.

³⁵ Article 8(1) of the 2003 MLAT. See Article 8(2) for the transmission of requests.

³⁶ FTC, Office of International Affairs, US Safe Web Act Information Sheet.

- any agency or judicial authority of a foreign government, including a foreign state, a political subdivision of a foreign state, or a multinational organisation constituted by and comprised of foreign states, that is vested with law enforcement or investigative authority in civil, criminal, or administrative matters;
- any multinational organisation, to the extent that it is acting on behalf of an entity as mentioned above.

On receiving a written request from a foreign law enforcement agency to provide assistance in accordance with this subsection, if the requesting agency states that it is investigating, or engaging in enforcement proceedings against possible violations of laws prohibiting fraudulent or deceptive commercial practices, or other practices substantially similar to practices prohibited by any provision of the laws administered by the Commission, other than Federal antitrust laws, the FTC will provide assistance without requiring that the conduct identified in the request constitute a violation of the laws of the US.

The FTC assistance can consist of:

- '(A) conduct such investigation as the Commission deems necessary to collect information and evidence pertinent to the request for assistance, using all investigative powers authorised by this Act; and*
- (B) when the request is from an agency acting to investigate or pursue the enforcement of civil laws, or when the Attorney General refers a request to the Commission from an agency acting to investigate or pursue the enforcement of criminal laws, seek and accept appointment by a United States district court of Commission attorneys to provide assistance to foreign and international tribunals and to litigants before such tribunals on behalf of a foreign law enforcement agency pursuant to section 1782 of title 28, United States Code.'*

In deciding whether to provide such assistance, the FTC must consider all relevant factors, including:

- '(A) whether the requesting agency has agreed to provide or will provide reciprocal assistance to the Commission;*
- (B) whether compliance with the request would prejudice the public interest of the United States; and*
- (C) whether the requesting agency's investigation or enforcement proceeding concerns acts or practices that cause or are likely to cause injury to a significant number of persons.'*

The US Safe Web Act of 2006 provides that '*If a foreign law enforcement agency has set forth a legal basis for requiring execution of an international agreement as a condition for reciprocal assistance, or as a condition for provision of materials or information to the Commission, the Commission, with prior approval and ongoing oversight of the Secretary of State, and with final approval of the agreement by the Secretary of State, may negotiate and conclude an international agreement, in the name of either the United States or the Commission, for the purpose of obtaining such assistance, materials, or information. The Commission may undertake in such an international agreement to:*

- (A) provide assistance using the powers set forth in this subsection;*
- (B) disclose materials and information in accordance with subsection (f) and section 21(b); and*
- (C) engage in further cooperation, and protect materials and information received from disclosure, as authorized by this Act'*³⁷.

Application of the US Safe Web Act of 2006 has been extended until 30 September 2027.

³⁷ Section 6 of the US Safe Web Act of 2006, on the sharing of information with foreign law enforcement agencies.

Again, it is quite clear that the US Safe Web Act of 2006 is not designed to tackle all kind of situations and its application is not unconditional. Rather, it was designed for important criminal cases and not for what could be perceived by the US as minor criminal cases.

The Data Protection Commissioner of Ireland and the Dutch Data Protection Authority have concluded MoUs with the FTC in the matter of the enforcement of laws protecting personal information in the private sector³⁸, referring e.g. to the US Safe Web Act of 2006.

2.2.3.4 The 2018 Clarifying Lawful Overseas Use of Data Act (the Cloud Act)

After several cases and legal disputes involving warrants to search data stored outside the US - notably in the EU³⁹ - the US adopted the 2018 Cloud Act.

In application of the 2018 Cloud Act, foreign governments may ask for the communication of data stored in the US when complying with several conditions, including the conclusion of an Executive Agreement with the US:

*'It shall not be unlawful under this chapter for a provider of electronic communication service to the public or remote computing service to intercept or disclose the contents of a wire or electronic communication in response to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523'*⁴⁰.

With respect to this, the US Department of State explains e.g. that:

- The Cloud Act aims to speed up access to electronic information held by US-based global providers that is critical to US foreign partners' investigations of serious crime, ranging from terrorism and violent crime to sexual exploitation of children and cybercrime;
- The Cloud Act is designed to permit US foreign partners that have robust protections for privacy and civil liberties to enter into bilateral agreements with the US to obtain direct access to this electronic evidence, wherever it happens to be located, in order to fight serious crime and terrorism;
- The Cloud Act authorises bilateral agreements between the US and trusted foreign partners that will make both nations' citizens safer, while at the same time ensuring a high level of protection of those citizens' rights.

To date, no executive agreement relating to the Cloud Act has been concluded between the US and the EU. It is not clear whether the EU is precluded from concluding this kind of executive agreement and if, in fact, such an agreement might only be possible between the US Government and each Member State acting separately⁴¹. In any case, the EU Commission has entered into negotiations for the conclusion of an EU-US agreement to facilitate access to electronic evidence in criminal investigations.⁴²

³⁸ Cf. https://www.ftc.gov/system/files/documents/cooperation_agreements/150309ftcdutchcb-1_0.pdf ; https://www.ftc.gov/system/files/documents/cooperation_agreements/130627usirelandmouprivacyprotection.pdf

³⁹ For example, the brief of the European Commission on behalf of the European Union as *Amicus Curiae* in support of neither party – United States of America v. Microsoft Corporation (US Court of Appeals, 2e Circuit), n° 17-2.

⁴⁰ US Code, Title 18, Chapter 119, Section 2511(2)(j).

⁴¹ On this point cf. e.g. Cassart, A., 'Premières réflexions sur le Cloud act: contexte, mécanismes et articulations avec le RGPD', Bruxelles, Larcier, *Revue du droit des technologies de l'information*, No. 73, 2018, p. 49.

⁴² Cf. <https://www.consilium.europa.eu/en/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/> and https://edpb.europa.eu/sites/default/files/files/file1/edpb_letter_out_2020-0054-uk-usagreement.pdf.

2.2.3.5 The Californian Uniform Foreign-Country Money Judgments Recognition Act

The Californian Uniform Foreign-Country Money Judgments Recognition Act only applies to foreign judgments that grant or deny recovery of a sum of money. However, it does not apply to a foreign-country judgment, even if the latter grants or denies recovery of a sum of money, to the extent that the judgment is a fine or any other penalty⁴³. Provision 1723 of the California Code of Civil Procedure (CCP) specifies that Chapter 2 does not prevent the recognition under principles of comity or otherwise of a foreign-country judgment not within its scope.

2.2.3.6 The California Consumer Privacy Act of 2018

In 2018, the State of California adopted the California Consumer Privacy Act⁴⁴. According to this act, the California Privacy Protection Agency is invested with full administrative power, authority, and jurisdiction to implement and enforce the California Consumer Privacy Act of 2018.

Among other things, the California Privacy Protection Agency shall '*Cooperate with other agencies with jurisdiction over privacy laws and with data processing authorities in other states, territories, and countries to ensure consistent application of privacy protections*'⁴⁵.

The California Privacy Protection Agency thus seems to be a natural correspondent for the EU SAs in the enforcement of their investigative and corrective powers.

2.2.3.7 Key findings

The enforcement of EU SAs' decisions in California courts may prove difficult if not impossible in a reasonable timeframe and without prejudice to its financial cost. However, the adoption of the California Consumer Privacy Act of 2018 may open the door to an active cooperation with the California Privacy Protection Agency.

2.2.4 The enforcement of SAs' investigative and corrective powers in the UK

This subsection presents a short introduction to the UK data protection legal framework and then considers different legal instruments that could support the enforcement of SAs' investigative and corrective powers.

2.2.4.1 UK Data Protection Legal Framework: DPA 2018 and the UK GDPR

The EU GDPR no longer applies to the UK. The UK Data Protection Act 2018 (DPA 2018) sets out the framework for the protection of personal data in the UK. It came into effect on 25 May 2018, and was amended on 1 January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the UK's status outside the EU.

The provisions of the EU GDPR have been incorporated into UK law as the UK GDPR. The DPA 2018 sits alongside and supplements the UK GDPR. The UK GDPR is a UK law which came into effect on 1 January 2021. It sets out the key principles, rights and obligations for most processing of personal data in the UK, except for processing by law enforcement and intelligence agencies.

The EU GDPR still applies to UK controllers/processors operating in the EEA, offering goods or

⁴³ California Code of Civil Procedure – CCP, Part 3. Of Special Proceedings of a Civil Nature, Title 11. Money Judgments of other jurisdictions, Chapter 2. Foreign-Country Money Judgments, §§1713-1725.

⁴⁴ State of California, Civil Code, Division 3. Obligations. Part 4. Obligations arising from particular transactions. Title 1.81.5. California Consumer Privacy Act of 2018, § 1789.199.10.

⁴⁵ Id., §1789.199.40(i).

services to individuals in the EEA, or monitoring the behaviour of individuals in the EEA. UK controllers/processors thus may need to comply with both the UK GDPR and the EU GDPR.

On 28 June 2021, the EU approved adequacy decisions for the EU GDPR and the Law Enforcement Directive (LED)⁴⁶. Both decisions are expected to remain in force until 27 June 2025.

The Information Commissioner's Office (ICO) (the UK Data Protection Supervisory Authority) states that it is not the regulator for any European-specific activities captured by the EU GDPR⁴⁷.

2.2.4.2 Selected ICO Commissioner functions and missions that could be of interest in the enforcement of EU SAs' investigative and corrective powers in the UK

(a) **Investigation on the basis of information received from a foreign authority**

According to Article 57(1)(h) of the UK GDPR, the Commissioner must '*conduct investigations on the application of this Regulation, including on the basis of information received from a foreign designated authority or other public authority*'.

(b) **Inspection on the basis of an international obligation of the UK**

According to Article 119(1) of the DPA 2018, '*The Commissioner may inspect personal data where the inspection is necessary in order to discharge an international obligation of the United Kingdom, subject to the restriction in subsection (2)*'.

*'The power under subsection (1) includes power to inspect, operate and test equipment which is used for the processing of personal data'*⁴⁸.

Excepted for urgent cases, '*the Commissioner must by written notice inform the controller and any processor that it intends to exercise power under subsection (1)*'⁴⁹.

(c) **International cooperation**

Article 120 of the DPA 2018 confers on the Commissioner a further international role in connection with the processing of personal data to which the UK GDPR does not apply.

For the processing of personal data to which the UK GDPR does apply, the DPA 2018 refers to Article 50 of the UK GDPR:

'In relation to third countries and international organisations, the Commissioner shall take appropriate steps to:

- (a) *develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;*
- (b) *provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;*
- (c) *engage relevant stakeholders in discussion and activities aimed at furthering*

⁴⁶ EU 28 June 2021 Decision on the adequate protection of personal data by the United Kingdom - General Data Protection Regulation; EU 28 June 2021 Decision on the adequate protection of personal data by the United Kingdom: Law Enforcement Directive.

⁴⁷ source: the ICO website.

⁴⁸ Article 119(3) of the DPA 2018.

⁴⁹ Article 119(4) and (5) of the DPA 2018.

- international cooperation in the enforcement of legislation for the protection of personal data;*
- (d) *promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.'*

2.2.4.3 UK MoUs in the field of data protection

The UK ICO has concluded several MoUs in the field of data protection⁵⁰:

- 2019 MoU between the Information Commissioner for the United Kingdom of Great Britain & Northern Ireland and Canadian Radio-television and Telecommunications Commission for cooperation in the enforcement of laws protecting personal data;
- 2019 MoU between the Personal Data Protection Commission of the Republic of Singapore and the Information Commissioner for the United Kingdom for cooperation in the enforcement of laws protection personal data;
- 2020 US FTC and UK ICO MoU on mutual assistance in the enforcement of laws protection personal information in the private sector;
- 2020 MoU between the Privacy Commissioner of Canada and the Information Commissioner of the United Kingdom on mutual assistance in the enforcement of laws protecting personal information in the private sector;
- 2020 MoU between the Privacy Commissioner for Personal Data of Hong Kong, China and the Information Commissioner for the United Kingdom for cooperation in protection personal data;
- 2020 MoU between the Information Commissioner for the United Kingdom of Great Britain & Northern Ireland and the New Zealand Department of Internal Affairs for cooperation in the regulation of unsolicited electronic messages;
- 2020 MoU between the Information Commissioner and the Global Cyber Alliance;
- 2021 MoU between the Information Commissioner for the United Kingdom of Great Britain & Northern Ireland and the Office of the Privacy Commissioner for New Zealand for cooperation in the enforcement of laws protecting personal data;
- 2021 MoU between the Information Commissioner for the United Kingdom of Great Britain & Northern Ireland and the National Privacy Commission of the Philippines for cooperation in the regulation of laws protecting personal data.

The content of these MoUs is not always strictly the same but some patterns are evident, such as sharing experience, investigative and enforcement assistance, and joint investigations. For instance, the MoU with the Canadian Radio-television and Telecommunications Commission covers sharing experience, exchanging information and joint investigations (excluding sharing personal data) but does not seem to be legally binding. The MoU with the US FTC covers the provision of investigative assistance in appropriate cases, sharing information, coordinating enforcement against certain cross-border privacy violations, etc. However, the assistance is not limitless, absolute or unconditional.

2.2.4.4 Enforcement of SAs' investigative and corrective powers falling within the scope of 'civil and commercial matters'

There is no indication from the answers received from the SAs to the questionnaire nor from the desk research whether SAs do or do not have the power to engage legal actions abroad either on the basis of Article 58(5) of the GDPR or under their national legislation. The answer to this question should be investigated under the rules governing the actions of the SAs including the possibility under the UK law for a foreign 'administrative' body to initiate legal actions in the UK.

⁵⁰ These MoUs can be found on the ICO website: <https://ico.org.uk/about-the-ico/our-information/working-with-other-bodies/>

In any case, if the enforcement of SAs' investigative and corrective powers is considered to fall within the scope of the notion of 'civil and commercial matters' (see section 2.2.1.2) (from a EU perspective) and accepted as such under UK law, EU SAs could consider the UK legal regime on recognition and enforcement of foreign judgments⁵¹ (see section 2.5.7 and section 2.2.1.2 for a discussion of whether SAs could be considered to act as private persons when they are not exercising 'public powers' under the accepted meaning in EU law, especially CJEU case-law analysis).

(a) International conventions or treaties in the matter of the recognition and enforcement of foreign judgments in the UK

The UK is a party to the Hague Convention on Choice of Court Agreements 2005 since 28 September 2020. As of the end of the Brexit transition period on 31 December 2020, however, it is no longer a party to the Lugano Convention 2007.

The UK is not a signatory to the Hague Convention on the recognition and enforcement of foreign judgments in civil and commercial matters 1971, nor to the Hague Convention on the recognition and enforcement of foreign judgments in civil or commercial matters 2019⁵².

The Hague Convention on Choice of Court Agreements 2005 does not seem an easy avenue to base a choice of jurisdiction between SAs and third-country controllers or processors.

(b) UK law on recognition and enforcement of foreign judgments

The Foreign Judgments (Reciprocal Enforcement) Act 1933 applies to judgments from courts in Australia, Canada (except Quebec and Nunavut), India, Israel, Pakistan, Guernsey, Jersey and the Isle of Man, and to judgments from some European countries (Austria, Belgium, France, Germany, Italy, the Netherlands, Norway).

Common law relating to the recognition and enforcement of foreign judgments applies where the jurisdiction from which the judgment relates does not have an applicable treaty in place with the UK or in the absence of any applicable UK statute. This typically refers to the US, China, Russia and Brazil. The addition of the EU to this list could be considered.

However, it is not clear whether any of these could support the enforcement of SAs' investigative and corrective powers in the UK.

2.2.4.5 Key findings

The enforcement of EU SAs' decisions in the UK courts may prove difficult - if not impossible - in a reasonable timeframe and without prejudice to financial cost. However, cooperation with the UK Data Protection Commissioner seems possible through the prism of Treaty 108+ (Articles 16 and 17), combined with the functions and missions vested in the UK Commissioner by the UK GDPR and DPA 2018. It is worth noting that the UK Commissioner has concluded a relatively high number of MoUs with foreign data protection authorities.

2.2.5 The enforcement of SAs' investigative and corrective powers in China

2.2.5.1 The Chinese legal framework in the matter of data protection

The Personal Information Protection Law (PIPL) was adopted on 20 August 2021 and will come into

⁵¹ On this topic, please cf. e.g. Cheshire, North & Fawcett, *Private International Law*, 15th ed., Oxford University Press, 2017; Browne, O. and Watret, T., *Enforcement of foreign judgments*, 10th ed., London, Law Business Research, Lexology, 2020.

⁵²

force on 1 November 2021. The PIPL should not be read in isolation but in combination with other Chinese laws that together comprise the Chinese data protection legal framework. Particular attention should be paid to the Data Security Law passed on 10 June 2021, which will come into force on 1 September 2021.

The scope for international assistance in the PIPL is not clear:

'If it is necessary to transfer personal information outside of China for international judicial assistance or administrative law enforcement, information handlers must file an application with the relevant competent authority for approval (Art. 41). The law stipulates that international treaties or agreements that China has become party to may govern cross-borders transfers and supersede the provisions of the law. It is not clear if this provision only concerns international judicial assistance, or also includes general cross-borders data transfers.'

The PIPL does not create an independent authority dedicated to its enforcement. Rather, the primary agency for data protection appears to be the Cyberspace Administration of China (CAC), but there are other regulators.

Of note is that in the event of a violation of the PIPL, the People's Procuratorates⁵³, and other relevant enforcing authorities may file a suit with a People's Court. However, at this stage, we have no information as to whether foreign authorities might ask for their cooperation or file a suit with a People's Court⁵⁴.

2.2.5.2 The recognition and enforcement of foreign judgments in China

The recognition and enforcement of foreign judgments in China might prove difficult:

*'In China, in theory, recognition and enforcement of foreign judgment ("REJ") are possible if there is, among other conditions, a treaty of mutual judicial assistance or reciprocity. Until recently, it was almost impossible to obtain REJ absent a treaty of mutual judicial assistance, which is rare and usually focused on criminal cases. However, lately, Chinese courts have shown more willingness to enforce foreign judgment on the basis of reciprocity and have adopted a pro-active attitude in triggering the reciprocity cycle'*⁵⁵.

There might be a need to establish some common grounds with Chinese values:

*'Beyond comity and reciprocity, the existence of shared values of privacy protection with the foreign jurisdiction and the legitimacy of the extraterritorial claim will significantly impact the likelihood of foreign enforcement. The more limited the nexus for jurisdiction is, the more likely it is that the foreign jurisdiction will not enforce the decision'*⁵⁶.

There might be unexpected consequences to the denial of recognising and enforcing foreign judgments:

*'Jurisdictional claims regarded as illegitimate (...) may even lead to the adoption of a "blocking statute". Such legislation may forbid the production of evidence or any documents in foreign proceedings, prohibit compliance with orders of foreign authorities, etc. (...)'*⁵⁷.

⁵³ The People's Procuratorates of the People's Republic of China are state organs for legal supervision.

⁵⁴ Dorwart, H., Zanfir-Fortuna, G. and Girot, C., 'China's new comprehensive data protection law: context, stated objectives, key provisions', *Future of Privacy Forum*, 20 August 2021; Greenleaf, G., *Asian Data Privacy Laws. Trade and Human Rights Perspectives*, Oxford University Press, 2017, pp. 218-219.

⁵⁵ Azzi, A., 'The challenges faced by the extraterritorial scope of the General Data Protection Regulation', *Journal of Intellectual Property, Information Technology and e-Commerce Law*, Vol. 9, No. 2, 2018, p. 66.

⁵⁶ Ibid., p. 67.

⁵⁷ Ibid., p. 68.

However, it seems that there could be some possibilities to enforce SAs' investigative and corrective powers to some extent:

*'In conclusion, cooperation with foreign jurisdiction may be relied on for the enforcement of the GDPR outside Europe to the extent that the jurisdictional claim is reasonable and legitimate (and with the consent of the State for investigation measures). It follows that it would probably require more than the mere utilisation of cookies to enforce a judgment abroad through the sole means of international cooperation'*⁵⁸.

2.2.5.3 Key findings

Cooperation with China seems possible in theory but would require a comprehensive approach, including close cooperation with EU and Member State public authorities responsible for the relationship with China.

2.3 IDENTIFICATION OF LEGAL INSTRUMENTS THAT COULD SUPPORT ENFORCEMENT OF THE GDPR

Section 2.3.1 presents the legal instruments that could support enforcement of the GDPR against a controller/processor, based on SAs' questionnaire responses. These legal instruments could be relied on when enforcing the GDPR against a controller/processor established in the US, UK or China that falls under Article 3(2), and in the recognition and enforcement of SAs' investigative and corrective powers.

Section 2.3.2 refers to other legal instruments, which, while not quoted by the SAs, could support enforcement of the GDPR against a controller/processor that falls under the scope of Article 3(2) GDPR but is not willing to cooperate with SAs and did not designate an EEA representative.

2.3.1 Legal instruments identified by SAs

2.3.1.1 Bulgarian SA

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications);
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) (for cooperation, assistance, decision notification);
- Personal Data Protection Act;
- European Convention on Human Rights (ECHR) (cooperation);
- Universal Declaration of Human Rights;
- Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime;
- Regulation 2019/788 (cooperation);
- Regulation 611/2016 (cooperation);
- Charter of Fundamental Rights (cooperation);
- Rules on the activity of the Commission for Personal Data Protection and its administration.

⁵⁸ Ibid., p. 69.

2.3.1.2 Finnish SA

- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) (for cooperation);
- Data Protection Act (1050/2018) (18a§) (cooperation in the framework of T108);
- Organisation for Economic Co-operation and Development (OECD) Guidelines (cooperation and mutual assistance).

2.3.1.3 French SA

The legal instruments that could be used with third countries to enforce the GDPR are either a legally binding agreement or a non-binding administrative arrangement (bilateral or multilateral) (Articles 46(3)(a) and 46(3)(b) of the GDPR).

However, under the French legal order, the French SA would not be able to use instruments labelled MoU, but could only conclude administrative arrangements (deriving from public international law and principles).

2.3.1.4 Italian SA

- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) (only for the UK).

2.3.1.5 Luxemburg SA

There is no specific legal instrument on which the Luxembourgish SA might rely. The national SA specified that international cooperation mechanisms with the US or other third-country officials under Article 50 GDPR are not yet concrete, either at EU or national level.

The national SA (CNPD) has no legal power under national law to initiate the drafting of a legally binding and enforceable instrument between public authorities or bodies with the objective of establishing an effective international cooperation channel⁵⁹ with guarantees for the transfer of personal data of the complainant to third countries⁶⁰.

The CNPD is limited by legal professional secrecy, as it cannot share information with other public entities unless those entities have similar professional secrecy obligations⁶¹.

At national level, only the government or parliament has the legal power to adopt legally binding and enforceable international instruments.

2.3.1.6 Polish SA

- Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community.

2.3.2 Other instruments to consider

Other instruments should also be considered as potentially supporting the enforcement of SA investigative and corrective powers abroad:

- Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018

⁵⁹ Article 50 GDPR.

⁶⁰ Article 46(2) of the GDPR.

⁶¹ Articles 42-44 of the Luxembourg Act of 1 August 2018.

- on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC;
- Articles 16 and 17 of the Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Treaty 108+), on Cooperation and Mutual Assistance: sharing of information, joint actions or investigations (compare with the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows (8 November 2001, ETS n° 181) (the UK has signed but not yet ratified Treaty 108+) (the US and China are not party to Treaty 108+);
- OECD 2007 Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy;
- OECD 2020 Summary of Discussion, 'Roundtable on Legislative Initiatives to Improve Cross-border Enforcement Cooperation' (DSTI/CP(2019)21/FINAL);
- OECD 2012 Background Note on Improving International Co-operation in Cartel Investigation (DAF/COMP/GF(2012)6));
- International Conference of Data Protection and Privacy Commissioners (ICDPPC), 2017 Global Cross-border Enforcement Cooperation Agreement, version 17);
- Global Privacy Enforcement Network 2013, Action Plan for the Global Privacy Enforcement Network (GPEN);
- Asia-Pacific Economic Cooperation (APEC) Cross-border Privacy Enforcement Arrangement (CPEA)

2.3.3 Key findings

There is not a clear view from the SAs' perspective on the legal instruments that could support the enforcement of the GDPR against third-country controllers and processors. However, it could be interesting to investigate further the effectiveness and efficiency of the GPEN while considering the experiences from the ICDPPC Enforcement Cooperation Agreement and the APEC Enforcement Arrangement. It is worth noting, for example, that the Office of the Australian Information Commissioner, the Office of the Victorian Information Commissioner, the New Zealand Office of the Privacy Commissioner, the US FTC, the Office of the Privacy Commissioner for Personal Data, Hong Kong, China, the Office of the Privacy Commissioner of Canada, are all CPEA participants.

2.4 SHARING SAs' EXPERIENCES AND IDENTIFICATION OF OTHER TYPES OF ACTIONS

Section 2.4.1 details the experiences reported by SAs in their answers to the questionnaire.

Section 2.4.2 describes other types of actions suggested by the SAs responding to the questionnaire, as well as other types of actions discussed in the legal literature.

2.4.1 Sharing SAs' experiences

2.4.1.1 Czech SA

In its previous investigations, controller/processor established in a country beyond the EEA zone always had a representative, in accordance with Article 27 of the GDPR. The Czech SA has yet to deal with a situation where it would be necessary to work directly with a controller/processor to enforce the GDPR.

2.4.1.2 Estonian SA

The Estonian SA received a request for assistance from a foreign data protection authority, asking it to provide investigation files of a case already decided by the Estonian courts. The request was deemed to be driven by political interests and the Estonian SA denied the request on the basis that there was no

legal ground for the demand.

2.4.1.3 Finnish SA

The Finnish SA's experience regarding entities outside the EEA that fall under Article 3(2) GDPR is limited to erasure requests from Google, for example, which did not require measures directly on the territory of a third country.

2.4.1.4 French SA (CNIL)

Two years ago, the CNIL was warned about the potential illegal collection of data on several websites and apps. It conducted online investigations and notified the data controller, which was established in the US. The CNIL then summoned the data controller to a hearing before its own department of investigation. The data controller attended the hearing and the proceeding is ongoing.

In a specific case where the CNIL could not clearly identify the data controller of a website but the data processor was identified as a Moroccan company, the CNIL asked its colleagues in the Moroccan data protection authority to perform an on-site investigation at the data processor's facility and inform the CNIL of its findings. The data controller was a company in Brazil and the CNIL chose not to continue the investigation as it would not have been able to enforce corrective powers on a Brazilian company.

In a third case, the CNIL received complaints about a major data breach concerning French data subjects (among others). It undertook an online investigation to confirm the data breach and lack of security. It then notified the data controller and asked several questions about the data breach. When the data controller failed to reply, the CNIL sent a letter to remind it of its legal obligations. The CNIL was not able to enforce its corrective powers.

In three separate cases, requests from non-European data protection authorities were handled informally via phone call or email exchanges. No information was disclosed, but the CNIL could advise the other authorities of the investigation and the stakes of the procedure in order to help them with their own investigations. The CNIL also discussed its method of investigation (e.g. how it conducts online investigations) and the tools used.

2.4.1.5 Croatian SA

The Croatian SA has only received inquiries from third countries about the interpretation of the provisions of the GDPR.

2.4.1.6 Italian SA

In 2015, in relation to some processing activities carried out by Google Inc. that fell under the scope of application of Article 4 Directive 95/46, the Italian SA sent a small team of IT and legal officers to the company headquarters in the US, on the basis of a verification protocol signed with the company and referenced in a decision adopted by the Garante in July 2014 to verify whether the measures implemented by the US controller were in compliance with Italian law.

The protocol envisaged quarterly updates on progress from the controller and empowered the Italian SA to carry out on-the-spot checks at Google's US headquarters. All information provided through progress updates or directly by the company during the on-the-spot check of the Garante was used to assess the implementation of the measures adopted by the Garante in its decision of 10 July 2014. The final decision of the Garante of 29 July 2016 is not available in English, however.

2.4.1.7 Lithuanian SA

The Lithuanian SA had no cases relating to a controller/processor established in the US, UK or China. It did, however, have a case regarding a controller established in Seychelles. The Lithuanian SA sent questions to a controller but no answers were provided and the case was dismissed. Although the GDPR application might be extraterritorial, the exercise of investigating powers against a controller/processor established outside the EU depends on the willingness of a controller/processor to provide answers.

2.4.1.8 Luxemburg SA

To date, the Luxembourg SA has only had experiences with entities established in the US. Considering its lack of effective enforcement powers on the US territory in practice, the SA usually makes informal contact with the controller/processor by post and email in order to try to reach a solution based on cooperation. Prior to that contact, it usually assesses whether it is possible to address the data protection issue with the controller/processor without disclosing any personal data. Where that is not possible (usually in the context of a complaint), the SA requests data subjects' consent under Article 49(a) GDPR to allow the transfer of their personal data in the US, in the absence of an adequacy decision pursuant to Article 45(3) GDPR or appropriate safeguards pursuant to Article 46 GDPR in national and EU law. Should the data subject refuse to consent, the SA is unable to process its complaint further. In some cases, the lack of effective enforcement powers of the SA makes it difficult to establish the applicability of Article 3(2) GDPR to the concerned entity, due to lack of available information or the possibility of obtaining that information if the concerned entity refuses to cooperate, in particular where the entity has not appointed a representative under Article 27 GDPR.

2.4.1.9 Polish SA

The Polish SA had some experience in sending requests for information to entities based in the US in the course of proceedings on complaints about violation of the provisions of the GDPR, specifically the transfer of personal data to the US without a legal basis (following the judgment of the CJEU in the Schrems II case).

For example, one of the organisations (private sector) conducted activities focused on European data subjects. This organisation is beyond the EEA. Under Article 58(1a) and (1e) of the GDPR, the Polish SA asked the organisation to answer the following questions: does the company have a representative for the processing of personal data in the EU, and if so, please provide its data? Who is the controller of personal data obtained from a controller's website? Whether the information is publicly available, and if so, please provide a precise indication? Does the company process personal data of citizens or other persons residing in the Republic of Poland? On what legal basis does the company process personal data of the above persons? What supervisory authority is mentioned in the privacy policy posted in the controller's website?

The US-based entity answered the authority's request as required. The entity's letter was drawn up in Polish, as required by Polish national law, and within the prescribed period. The entity appointed a proxy (legal attorney – resident of Poland) to represent the controller before the President of the Personal Data Protection Office.

2.4.1.10 UK ICO

In 2018, the UK ICO served a first enforcement notice to the company AIQ Ltd., which had no physical presence in the EU (known as the Cambridge Analytica scandal). The notice was based on Article 3(2) of the EU GDPR. The notice required AIQ Ltd. to cease processing any personal data of EU citizens obtained from organisations or otherwise, for the purposes of data analytics, political campaigns or any advertising purposes. The scope of the second notice was narrowed to individuals in the UK. AIQ Ltd. was given 30 days to comply before facing a fine of EUR 20 million or 4% of its global turnover,

whichever was the higher.

2.4.2 Identification of other types of action and SAs' observations

2.4.2.1 Other types of action suggested by SAs

(a) Bulgarian SA

The Bulgarian SA stated that the current system of rules and procedures, together with experience and administrative capacity, should create enough safeguards to ensure enforcement of the GDPR provisions.

(b) French SA

An efficient measure would be for SAs to order the internet service providers within their jurisdiction to deny access to a particular domain name (or to redirect connections to a warning page).

(c) Croatian SA

Raising awareness among all controllers, including those from third countries that provide their services to data subjects in the EEA.

(d) Italian SA

The Garante does not have the power to order an internet connectivity service provider to inhibit access from Italy to websites collecting personal data unlawfully (this power was recently conferred on the Italian authority responsible for regulating the Italian financial markets (Consob) in cases where financial services are offered without due authorisation), but this power could perhaps be useful.

An order to stop collecting/processing personal data by means of a website could be adopted by the SA as one of the corrective measures under Article 58(2) of the GDPR. Like the other corrective measures, however, it will be difficult to enforce in respect of an Article 3(2) controller/processor.

(e) Polish SA

Imposition of the restriction of processing of personal data of EU citizens.

(f) Slovakian SA

The Slovakian stated that effective enforcement needs an entity in the EEA against which the SA could exercise the corrective powers in the territory where this entity is established or has a representative.

2.4.2.2 Other types of action suggested in the legal literature

Other types of action are suggested in the legal literature:

- Asset-freezing orders when controllers/processors possess assets in the EU⁶²;
- 'Market destroying measures' to penalise the operator (prohibiting the party from trading within the jurisdiction or making debts owed to that party unenforceable within the

⁶² Azzi, A., 'The challenges faced by the extraterritorial scope of the General Data Protection Regulation', *Journal of Intellectual Property, Information Technology and e-Commerce Law*, Vol. 9, No. 2, 2018, p. 70.

- jurisdiction)⁶³;
- Obtaining a court injunction against the local business partners that are indirectly using the processed personal data⁶⁴;
- Obtaining a court injunction blocking the websites of the operator or its partners, or the associated internet connections (via injunctions applied to internet service providers)⁶⁵;
- Encouraging codes of conduct⁶⁶.

The legal literature reported that the Belgian SA has concluded an agreement with a not-for-profit private association that registers domain names. Under that agreement, the association will enforce the Belgian SA's decision to block internet sites with a (.be) extension.

2.4.3 Key findings

SAs have gained some experience of international cooperation, albeit informally. They identified some avenues to improve international cooperation in data protection. Direct action against the electronic communications infrastructure or the intermediaries located in EEA territories (e.g. order to stop collecting personal data or order to shut down a website) appears to be most effective.

2.5 ANALYSIS OF THE POSSIBILITY TO RELY ON UNILATERAL COMMITMENTS FROM CONTROLLERS/PROCESSORS IN THE MATTERS OF CHOICE OF JURISDICTION AND APPLICABLE LAW

This subsection analyses the possibility to rely on controllers'/processors' commitments in the matters of choice of jurisdiction and applicable law, based on the existence of a mutual agreement, a clause in BCR, or a unilateral commitment from controllers/processors.

The validity of controllers/processors commitments established in California or the UK is analysed through the prism of EU law but not US/California law or UK law. The information for this section is drawn from SAs' responses to the questionnaire.

Sections 2.5.1 – 2.5.3 discuss the choice of jurisdiction in an agreement between a controller/processor from a third country and an EEA SA (Section 2.5.1), in the BCR (Section 2.5.2), and in a unilateral commitment from the controller/processor (Section 2.5.3).

Sections 2.5.4 – 2.5.6 discuss the choice of applicable law in case of an agreement (Section 2.5.4), BCR (Section 2.5.5) or unilateral commitment (Section 2.5.6).

Finally, **Section 2.5.7** describes the impact of the CJEU's interpretation of the notion of 'civil and commercial matters' where that notion could apply to EEA SAs exercising their powers abroad.

2.5.1 Possibility for an agreement between controllers/processors and SAs on choice of jurisdiction

SAs did not recognise the possibility of an agreement with controllers/processors on the choice of jurisdiction.

The French SA observed that '*Since we are in a 3(2) scenario, the European framework does not allow for a choice of jurisdiction as this is covered directly by the GDPR. Therefore, private international law principles cannot apply in this case.*'

⁶³ Ibid., p. 72.

⁶⁴ Ibid., p. 73.

⁶⁵ Ibid., p. 73.

⁶⁶ Ibid., p. 78 et seq.

The Italian SA considered that ‘*Article 78.3 GDPR already identifies the relevant jurisdiction for proceedings against an SA and we are not sure the SA may “derogate” from this provision.*’

2.5.2 Possibility to rely on a choice of jurisdiction in BCR

SAs’ responses in respect of the possibility to rely on a choice of jurisdiction in BCR were more diverse. It seems possible for the Bulgarian, the Finnish and the Italian SAs (to some extent), but not possible for the Czech and French SAs (the latter for the same reasoning as in Section 2.5.1).

However, the Italian SA specified that, ‘*According to Article 47.2.e GDPR, an EEA SA will be competent for complaints lodged with it by a data subject for cases where a violation of the BCRs has been carried out by a third country BCR member, i.e. the third country BCR member accepts an EEA SA’s and/or court’s jurisdiction for such cases. By the same token, for example, they accept to comply with any EEA competent SA’s decision or advice relating to compliance with/interpretation of the BCRs. BCRs cannot contain provisions according to which a SA shall accept any other jurisdiction than its own. With regard to the enforcement against an Article 3.2 controller/processor, the jurisdictions referred to in the BCRs could be relevant only for cases where the SA will have to assess compliance with the commitments contained in the BCR for transfers and onward transfers carried out by the same Article 3.2 controller/processor.*’

2.5.3 Possibility to rely on a choice of jurisdiction in a unilateral commitment from controllers/processors

Most of the SAs that responded to the questionnaire did not recognise the possibility of a choice of jurisdiction in a unilateral commitment from controllers/processors (the French SA repeating the same reasoning as in Section 2.5.1).

However, the Italian SA considers that ‘*BCRs, commitments taken by means of unilateral declarations can be taken into account only under certain conditions specified in the WP 256 and 257 (BCR Referentials). This also applies to the commitment to accept the jurisdiction of the Italian SA and/or an Italian court.*’

2.5.4 Possibility for an agreement between controllers/processors and SAs on choice of the applicable law

Most of the SAs that responded to the questionnaire did not recognise the possibility of an agreement between controllers/processors and SAs on the choice of applicable law (the French SA repeating the same reasoning as in Section 2.5.1).

2.5.5 Possibility to rely on a choice of applicable law in BCR

Most of the SAs that answered the questionnaire did not recognise the possibility to rely on a choice of applicable law in BCR (the French SA repeating the same reasoning as in Section 2.5.1).

However, the Italian SA noted that ‘*We can rely on the choice made by a third-country BCR member to accept the Italian law as the one applicable to their processing of personal data transferred from the Italian territory under the BCRs.*’

2.5.6 Possibility to rely on choice of applicable law in a unilateral commitment from controllers/processors

With the exception of the Italian SA, most of the SAs that responded to the questionnaire did not recognise the possibility to rely on a choice of applicable law in a unilateral commitment from controllers/processors (the French SA repeating the same reasoning as in Section 2.5.1).

2.5.7 Impact of CJEU interpretation of the notion of 'civil and commercial matters'

Situations where SAs are not exercising public powers when exercising their investigative and corrective powers (see Section 2.2.1.2) could be within the scope of the notion of 'civil and commercial matters'. The application of Regulation (EU) No 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, as well as Regulation (EC) No 593/2008 on the law applicable to contractual obligations (Rome I), could therefore be considered.

If this possibility is confirmed, SAs and controllers/processors could rely on Article 25(1) of the Regulation No 1215/2012 to agree on a choice of jurisdiction, the latter providing that:

'If the parties, regardless of their domicile, have agreed that a court or the courts of a Member State are to have jurisdiction to settle any disputes which have arisen or which may arise in connection with a particular legal relationship, that court or those courts shall have jurisdiction, unless the agreement is null and void as to its substantive validity under the law of that Member State. Such jurisdiction shall be exclusive unless the parties have agreed otherwise. (...)'

Similarly, SAs and controllers/processors could rely on Article 3 Regulation No 593/2008 to agree on the applicable law. This choice is not necessarily limitless or unconditional (please cf. Article 3(3-5)).

2.5.8 Key findings

It appears quite difficult for SAs to rely on unilateral commitments from controllers and processors on the choice of jurisdiction or applicable law. However, if SAs are to be considered as acting in 'civil and commercial matters', there could be some discussion about the possibility for some degree of choice of jurisdiction or applicable law.

2.6 IMPORTANCE OF CONTROLLER/PROCESSOR REPRESENTATIVES

This subsection analyses the added value and limits of controllers/processors' representatives, as perceived by SAs (see **Section 2.6.1** and **Section 2.6.2**, respectively). The analysis is based on SAs' responses to the questionnaire and includes their experiences with EEA representatives (**Section 2.6.3**). **Sections 2.6.4** discusses the scope of representatives' obligations under the GDPR.

2.6.1 Added value of controller/processor representatives in the experience of SAs

The majority of the SAs that responded to the questionnaire underlined the importance of the designation of a representative for controllers/processors that fall under the scope of Article 3(2) GDPR. They stressed that:

- The representative provides a direct link to the controller, acts as a contact point for SAs (e.g. notification of a corrective measure) and data subjects, and facilitates communication (BG, FI, FR, HR, HU, IT, PL);
- The representative may be addressed in addition/instead of the controller/processor by the SA on all issues related to processing, for the purposes of ensuring compliance with the GDPR. The powers of the SA may be exercised against the representative in the Union (LT, SK);
- When SAs order controllers to bring data processing into compliance with the GDPR or decide to impose a fine, the representative should provide SAs with information on the enforcement of these decisions (FR);
- The representative facilitates the exercise of data subjects' rights (BG);
- There is a possibility to enforce investigative and corrective powers on the representative (LU);

- The designation of a representative is crucial because it is not possible to initiate an audit against a controller/processor outside the EEA if there is no representative within the EEA (SE).

2.6.2 Limits to the added value of controller/processor representatives as perceived by SAs

SAs highlighted some limits to the perceived added value of controllers' representatives:

- The possibilities for enforcement against representatives are limited. In line with Recital 80 and Article 27(5) of the GDPR, the designation of a representative in the Union does not affect controllers/processors' responsibility and liability and shall be without prejudice to legal actions that could be initiated against the controller/processor themselves. The GDPR does not establish a substitutive liability of the representative in place of the controller/processor it represents in the Union (cf. EDPB Guidelines, 3/2018) (FI);
- Any possibility to address corrective measures - in particular, administrative fines - to the representative should be further explored, taking into account that it merely 'represents' the Article 3(2) controller/processor (IT).

2.6.3 SAs' experiences of controller/processor representatives

2.6.3.1 Italian SA

To date, the Italian SA has carried out two investigations by contacting the representatives of two companies established in third countries and receiving the cooperation and information it requested.

One case related to a representative designated by a Swiss company in the EEA according to Article 27 of the GDPR. The company processed personal data of Italian data subjects for anti-money laundering purposes. The representative also acts as the company's data protection officer and cooperated fully. The case is ongoing.

Another investigation concerned a Turkish company processing personal data of persons in Italy by means of a website, which designated a representative in the Netherlands. The company granted the data subjects' requests by means of its representative and the case was closed by the Italian SA.

Two ongoing cases relate to controllers under Article 3(2) of the GDPR. They were initiated directly against the controllers as no representatives have been designated (both companies challenge the applicability of the GDPR). The Italian SA notified the controllers, according to Section 166.5 of the Italian Data Protection Code, of the alleged violations, pursuant to the safeguards set out in the Garante's Internal Regulations (cf. also Section 166.9) and are waiting on a reply from the companies. No enforcement actions relating to final decisions of the IT SA have begun.

2.6.3.2 Slovenian SA

The Slovenian SA has initiated one case against an information service provider from the US with a representative in Slovenia. The case is still pending. In the inspection procedure, the SA requested information from the data controller via its representative, and replies were provided in due time.

2.6.4 Legal analysis of the scope of representatives' obligations under the GDPR

The EDPB 3/2018 Guidelines on the territorial scope of the GDPR (Article 3) (version 2.1) highlights the eight following elements that are relevant to the analysis of the scope of representatives' obligations under the GDPR, with respect to the enforcement of SAs' investigative and corrective powers:

- Article 3(2) of the GDPR: data controllers/processors are under the obligation to name a representative in the Union;
- The presence of a representative in the Union does not constitute an ‘establishment’ for the controller/processor on the basis of Article 3(1) of the GDPR;
- The representative in the Union acts on behalf of the controller/processor it represents with regard to its obligations under the GDPR;
- While not itself responsible for complying with data subject rights, the representative must facilitate communication between data subjects and the controller/processor in order to give effect to the exercise of data subjects’ rights;
- The controller/processor’s representative shall maintain a record of processing activities under the responsibility of the controller/processor. It is the representative’s own responsibility to be able to provide that record when requested by an SA;
- The representative should perform its tasks according to the mandate received from the controller/processor, including cooperating with the competent SAs on any action taken to ensure compliance with the GDPR. Accordingly, the representative should be able to facilitate any information or procedural exchange between a requesting SA and an Article 3(2) of the GDPR controller/processor. The representative in the Union must therefore be in a position to efficiently communicate with data subjects and cooperate with the SAs concerned;
- The designation of a representative in the Union does not affect the responsibility and liability of the controller/processor under the GDPR and shall be without prejudice to legal actions that could be initiated against the controller/processor themselves;
- The GDPR does not establish substitutive liability of the representative in place of the controller/processor it represents in the Union.

In addition, the EDPB rightly recalls that ‘*(...) the concept of the representative was introduced with the aim of facilitating the liaison with and ensuring effective enforcement of the GDPR against Article 3(2) of the GDPR controllers/processors. To this end, it was the intention to enable supervisory authorities to initiate enforcement proceedings through the representative designated by the controllers or processors not established in the Union. This includes the possibility for supervisory authorities to address corrective measures or administrative fines and penalties imposed on the controller or processor not established in the Union to the representative, in accordance with articles 58(2) and 83 of the GDPR. The possibility to hold a representative directly liable is however limited to its direct obligations referred to in Article 30 and Article 58(1)a of the GDPR.*

However, it should be underlined that GDPR Recital 80 specifies *in fine* that ‘*(...) The designated representative should be subject to enforcement proceedings in the event of non-compliance by the controller or processor.*’ With respect to this point, Azzi wrote in 2018 that:

‘There is much controversy as to whether a representative may incur some sort of liability, in addition to the operator, and no guidance has been issued by the Art. 29 WP. Meanwhile, as the first Member State to have implemented the regulation, Germany has interpreted this provision law as enabling civil law proceedings to be directed against the representative. Further, in a recent case against WhatsApp, held under the directive, the Netherlands has considered that the DPO could incur liability in case of non-compliance with the directive, despite this not being specified by the directive. In response, WhatsApp claimed that it could not find any officer ready to endorse such liability, but the “impossibility” argument has been rejected. The Dutch court added that the parties could agree in contract to indemnify the officer in case of liability. Besides, the IAPP, a non-profit organisation which share best practices for privacy management issues, has also interpreted Article 27 of the regulation in this sense: “it seems likely the EU representative would be required to at least initially incur the legal and other costs for addressing enforcement actions and be responsible for paying administrative fines and damage suit awards”.

‘From those observations and considering the influence that may have the first implementation

law on other Member States, there is a real possibility for representatives to be subject to enforcement measures. Of course, the law would be more effective if such power of coercion could be exercised locally. Besides, it would reduce the costs inherent to cross-border litigation.'

'However, a number of objections temper this possibility. First, as it was claimed by WhatsApp, operators might encounter a real difficulty in finding a representative eager to incur a potentially significant liability. Second, a representative may not actually have much influence over the foreign operator and may not have sufficient financial or material means to deal with the sanctions. Finally, even though the obligation to appoint a representative is sanctioned by a fine of up to 2% of the global turnover, there might well be some operators who decide to ignore it and not respond to any sanctions.'

Millard and Kamarinou (2020) considered that Article 27 did not impose any direct liability on representatives. But they highlighted the wording of Recital 80⁶⁷. They appear to suggest the possibility that Article 27 could be interpreted as allowing SAs to initiate legal proceedings against representatives. With respect to this, they highlight the fact that, e.g. Article 30 of the Spanish Organic Law 3/2018 of 5 December 2018 on the protection of personal data and safeguarding of digital rights provides that:

1. *In the cases in which Regulation (EU) 2016/679 applies to a controller or processor not established in the European Union under Article 3(2) thereof and the processing refers to data subjects found in Spain, the Spanish Data Protection Agency or, where appropriate, the regional data protection authorities, may impose the measures established in Regulation (EU) 2016/679 on the representative, jointly with the controller or processor.*
This requirement shall be without prejudice to the liability that could, where appropriate, be borne by the controller or processor and to the exercise by the representative of action under a right of recourse against the relevant party.
2. *Moreover, in case of liability in the terms provided for in Article 82 of Regulation (EU) 2016/679, the controllers, processors and representatives shall be jointly liable for the damage caused.'*

In a 2021 update, the authors stated that:

'(...) the EDPB has confirmed that under the GDPR representatives are not liable for infringements of the controller or processor they represent but only for the obligations addressed directly to representatives in Articles 30 and 58(1) of the GDPR. As the nature of the role of representatives is to be a point of contact in the Union for the controller or processor not established in the Union and to facilitate enforcement proceedings against such controllers or processors, it follows that the intention of the GDPR was to "enable supervisory authorities to initiate enforcement proceedings through the representative". In practice, this means that supervisory authorities may "address corrective measures or administrative fines" imposed on controllers or processors not established in the Union to representatives but without holding representatives directly liable for such measures or fines. Representatives act only as a liaison between supervisory authorities and the controllers or processors they represent.'

It is our current view that, in addition to the EDPB 3/2018 Guidelines regarding the scope of representatives' obligations under the GDPR, it should be considered that:

- SAs should be entitled to send all notifications directed to controllers/processors to the

⁶⁷ Millard, Chr. and Kamarinou, D., 'Article 27. Representatives of controllers or processors not established in the Union', in Chr. Kuner, Lee A. Bygrave and Chr. Docksey, *The EU General Data Protection Regulation (GDPR). A Commentary*, Oxford University Press, 2020, p. 597; the *Update of Selected Articles. Covering developments between 1 August 2019 and 1 January 2021*, May 2021.

representative's physical address in the EU, including orders directed to controllers/processors to appear before SAs' Office or courts. This would mean that there is no need to realise any other sort of notifications notably in the third country where the controller/processor is established;

- Controllers/processors' representatives could be sued by SAs when not acting according to their obligations under the GDPR. This raises the question as to whether it would be possible for SAs to sue representatives for not acting according to their contractual obligations vis-à-vis the controller/processor, as well as the question as to the scope of their liability.

It also raises the question as to whether national legislation could go beyond the GDPR regime in respect of the scope of controllers/processors' representatives' liability.

2.6.5 Key findings

It is clear that the appointment of a controller/processor representative is crucial to the enforcement of SAs' investigative and corrective powers. non-compliance with Article 27 GDPR should be punished under Article 83(4)a of the GDPR (administrative fines).

2.7 INTERNATIONAL COOPERATION FORESEEN IN THE GDPR (ARTICLE 50)

This subsection presents the obstacles that SAs identified in international cooperation in the field of data protection (Section 2.7.1), as well as possible solutions (Section 2.7.2). It also presents SAs' experiences with third countries cooperating on data protection and/or recognising SAs' investigative or corrective powers, and MoUs concluded by some SAs (Sections 2.7.3 and 2.7.4, respectively). It closes with a short consideration of EU trade agreements and the enforcement of SAs' investigative or corrective powers (Section 2.7.5).

2.7.1 Main obstacles to international cooperation in the field of data protection identified by SAs

In their questionnaire responses, SAs identified several obstacles to international cooperation in the field of data protection:

- Differences between national legislations (BG, IT, SK);
- Differences between SAs' procedural regimes (BG, FI, IT, SK);
- Absence of data protection law in third countries (PL);
- General understanding of data protection rules (BG);
- Lack of practice (EE);
- Determining relevant interlocutors in the third country (IT);
- Anonymity of website owners (FI);
- Enforcement of fines/orders (FI);
- Impossibility of producing findings when the data controller is outside the SA's national borders, does not have a website, and refuses to answer SAs' questions or appear for a hearing (FR);
- In exercising their corrective powers, SAs have no way to ensure that the decision would be enforced abroad if the data controller chooses not to comply (FR);
- Under-capacity (small number of employees) (HR);
- Slow pace of administration (HU);
- Probative force of documents collected by another authority in a different jurisdiction (IT);
- Language difficulties (HU, IT);
- Absence of any legally binding and enforceable instrument between public authorities or bodies to establish an effective international cooperation channel and provide guarantees for the transfer of personal data of the complainant to third countries (LU, PL);
- Non-effective (or non-existent) procedures regarding enforcement of the GDPR abroad (PL);

- Non-recognition by the US of European standards on the protection of personal data (in particular, the processing of personal data by US national security protection authorities) (PL).

2.7.2 Tools to improve international cooperation in the field of data protection identified by SAs

SAs identified several tools to improve international cooperation in the field of data protection:

- Stronger international voluntary initiatives, such as the Global Privacy Assembly (BG, FR, LU);
- Guidance with practical examples (EE);
- International agreements in the field of data protection (FI, PL);
- International agreements, MLAT, or administrative arrangements (IT);
- Means to enforce a decision made by an EU SA outside the EU (FR);
- Tools to frame international cooperation (administrative arrangements or international agreements), providing support to the enforcement of SAs decisions and sanctions in third countries and, to the extent possible, to shared investigative actions and appropriate safeguards (FI, FR, IT, PL, SI, PL);
- Issuing of more adequacy decisions (PL);
- Better and more developed communication systems and tools (HR);
- Tools enhancing the pace of administration and supporting translation (HU);
- Ability for several SAs to join a formal request addressed to another SA outside the EU (FR);
- Some cooperation at EDPB level (e.g. template international agreements or administrative arrangements (FR, IT, PL).

2.7.3 Identification of third countries that would cooperate on data protection and/or recognise SAs' investigative or corrective powers

The **French SA** stated that some third countries offer their cooperation depending on whether the offences are recognised in that country. However, they consider it difficult to put in place a formal cooperation considering the different legal frameworks in place. Cooperation with some third countries thus remains informal.

The **Italian SA** and Albanian Data Protection Authority entered into a **Cooperation Agreement** on 10 February 2015. The Agreement envisages joint inspection activities at both public administrative bodies and private entities, including call centres operating in Albania. The underlying objectives include the exchange of experience and know-how, handling of complaints lodged by citizens of either country, provision of support in drafting reports and analyses, and regulatory updates. In 2017, on the basis of this Cooperation Agreement, the **Italian SA** (with a small team of legal and IT experts) participated in an inspection activity by the Albanian Data Protection Authority at two call centres in Albania. This cooperation allowed the Garante to share its expertise on inspection procedures, with a view to fostering enforcement of the Albanian data protection legislation in a sector that often involves processing Italian data subjects' personal data for telemarketing purposes.

2.7.4 MoUs

Some SAs concluded MoUs⁶⁸ under the previous EU data protection regime:

- 2012 MoU between the Privacy Commissioner of Canada and the Federal Commissioner for Data Protection and Freedom of Information of **Germany** on mutual assistance in the enforcement of laws protecting personal information in the private sector;
- 2014 MoU between the Privacy Commissioner of Canada and the Data Protection

⁶⁸ <https://www.priv.gc.ca/en/about-the-opc/what-we-do/memorandums-of-understanding/>

Commissioner of **Ireland** on mutual assistance in the enforcement of laws protecting personal information in the private sector;

- 2014 MoU between the Privacy Commissioner of Canada and the College Bescherming Persoonsgegevens (the **Netherlands**) on mutual assistance in the enforcement of laws protecting personal information in the private sector;
- 2014 MoU between the Privacy Commissioner of Canada and the National Supervisory Authority for Personal Data Processing of **Romania** on mutual assistance in the enforcement of laws protecting personal information in the private sector.

2.7.5 Enforcement of SA investigative and corrective powers in EU trade agreements

There are no effective mechanisms for the enforcement of SAs' investigative and corrective powers in the trade agreements concluded by the EU:

- EU-Singapore Free Trade Agreement, 19 October 2018;
- EU-Vietnam FTA, 30 June 2019;
- EU-Canada Comprehensive Economic and Trade Agreement (CETA), 21 September 2019;
- EU-China Comprehensive Agreement on Investment, 30 December 2020;
- EU-UK Trade and Cooperation Agreement, 30 December 2020.

Nor are there such mechanisms in the texts under negotiation:

- EU-Mercosur Trade Agreement;
- EU-Mexico Trade Agreement;
- EU-Australia Trade Agreement;
- EU-New Zealand Trade Agreement⁶⁹.

2.7.6 Key findings

Strengthening international cooperation seems the best avenue for better and easier enforcement of SAs' investigative and corrective powers against third-country controllers/processors that fall under the scope of Article 3(2) of the GDPR but are not willing to cooperate with SAs and did not designate an EEA representative. In the short term, the conclusion of MoU (or equivalent) should be considered. The use of legal instruments in the matter of criminal cooperation (e.g. MLAT) could be considered where there is a serious breach of the GDPR that amounts to a criminal offence. Finally, closer cooperation with the EU Commission when the latter is negotiating trade agreements could be useful in creating effective mechanisms to enforce SAs' investigative and corrective powers abroad.

⁶⁹ See also the 2016 Enhanced Partnership and Cooperation Agreement between the European Union and its Member States, of the one part, and the Republic of Kazakhstan, of the other part, article 237

3 CONCLUSIONS

This Study aimed to analyse the possibilities available to enforce SAs' investigative and corrective powers against third-country controllers/processors that fall under the scope of Article 3(2) of the GDPR but are not willing to cooperate with SAs and did not designate an EEA representative. The analysis focused on controllers and processors established in California (US), the UK, and (to the extent possible) China. The analysis was based on desk research and SAs' responses to a survey of their experience with enforcement in third countries. The main findings of the Study are as follows.

(a) Possibility to summon third-country controllers/processors to appear before SA's Office, or in the SA's national courts or tribunals

SAs do not seem to have the same kind of powers to summon third-country controllers/processors to appear before their Offices or in Courts. We know that Article 58(5) of the GDPR may be used by SAs as soon as the GDPR applies to the controller; however, as SAs must exercise their powers on their national territory, it is not clear whether this precludes SAs initiating legal proceedings in another Member State or in a third country on basis of Article 58(5) of the GDPR. Equally unclear is the position of the CJEU regarding the lack of any kind of establishment of the controller/processor on the territory of any Member State in respect of the possibility to open any 'international jurisdiction or competence' to the benefit of any 'court or tribunal' of the Member State of the SA on the basis of Article 58(5) of the GDPR. In our view, SAs should be entitled to summon a third-country controller/processor that falls within the scope of Article 3(2) GDPR but is unwilling to cooperate with SAs and did not designate an EEA representative to appear before their Office, or in the SA's national courts or tribunals.

(b) Enforcement of SAs' investigative and corrective powers in California, the UK and China

SAs do not qualify as 'courts or tribunals' in the meaning of Article 267 of the TFEU when exercising their investigative and corrective powers, and SAs should be considered to exercise 'public powers' under European law only when making use of special powers that go beyond those arising from the ordinary legal rules applicable to relationships between private individuals. With respect to this, the wording of Article 58 of the GDPR might be slightly misleading as to the nature of these powers (e.g. Article 58(1)c, e, f; Article 58(2)a, b, c, d, e, g). If SAs are not considered to exercise 'public powers' as understood under EU law, there is a possibility that SAs could be considered as acting like 'private persons' in 'civil and commercial matters' (e.g. in the field of international jurisdiction and applicable law). In consequence, the very nature of those powers could have to be additionally ascertained in light of the powers conferred on SAs by their national data protection laws.

In theory, SAs may exercise their investigative and corrective powers in a manner that produces effects beyond the EEA territories within the framework of the relevant international law. However, that does not necessarily imply that:

- Third countries will accept SAs exercising investigative and corrective powers in a manner that produces effects on their territories;
- third countries will accept SAs initiating legal actions or proceedings before their courts or tribunals;
- third countries will recognise that SAs are acting in 'civil or commercial matters' or that they are exercising 'public powers';
- the rules applied by SAs when exercising their investigative and corrective powers are 'acceptable' or 'applicable' in the third countries' courts or tribunals;
- SAs are allowed to send agents abroad to third countries, even with the consent of the controllers/processors established in those countries.

It results from the findings that the enforcement of EU SAs' decisions in California and UK courts may

prove difficult - if not impossible - in a reasonable timeframe and without prejudice to its financial cost. However, the adoption of the California Consumer Privacy Act of 2018 may open the door to active cooperation with the California Privacy Protection Agency. Similarly, cooperation with the UK Data Protection Commissioner seems possible to consider through the prism of Treaty 108+ (Articles 16 and 17), combined with the functions and missions imparted to the UK Commissioner by the UK GDPR and DPA 2018. It is worth noticing that the UK Commissioner has concluded a relatively high number of MoUs with foreign data protection authorities. Cooperation with China seems possible in theory but would require a comprehensive approach, including close cooperation between the EU and the Member State public authorities responsible for the relationship with China. Cooperation with the US through the 2003 MLAT or the US Safe Web Act of 2006 is not impossible but is designed for large criminal cases. Nor is that cooperation limitless or unconditional. Cooperation through the Cloud Act does not seem any simpler.

Effective international cooperation seems to require a similarity of approach and enforcement mechanisms – similar to the traditional notion of reciprocity.

(c) Identification of legal instruments supporting enforcement of SAs' powers

The SAs identified legal instruments that could support enforcement of the GDPR against third-country controllers/processors. The Study highlights some additional instruments that could also usefully be considered.

(d) Sharing SAs' experience and identifying other types of actions

In practice, SAs have some experience of international cooperation, albeit more informally. International cooperation between EU SAs and foreign data protection authorities raises the issue of the appropriate safeguards needed for transferring personal data of data subjects to foreign data protection authorities.

SAs identified some avenues to improve international cooperation in the field of data protection. Direct action on the electronic communications infrastructure or the intermediaries located on the EEA territories (e.g. order to stop collecting personal data or order to shut down websites) seems the most effective.

(e) Possibility to rely on controller/processor unilateral commitments on choice of jurisdiction and applicable law

It seems difficult to effectively rely on commitments from controllers/processors on the choice of jurisdiction or applicable law. However, if SAs are considered to act in ‘civil and commercial matters’, there could be some room for a degree of choice of jurisdiction and applicable law.

(f) Importance of the appointment of controller/processor representative

The appointment of a controller/processor’s representative is crucial to the enforcement of SAs’ investigative and corrective powers, even if, ultimately, the representative will not pay for the controller/processor’s liability.

(g) Main obstacles to international cooperation in the field of data protection

SAs identified several obstacles to international cooperation in the field of data protection, such as a lack of practice, shortcomings in the legal framework, and problems in producing evidence.

In conclusion, strengthening international cooperation seems to be the best avenue for better and easier enforcement of SAs’ investigative and corrective powers against third-country controllers/processors that fall under the scope of Article 3(2) of the GDPR but are not willing to cooperate with SAs and did

not designate an EEA representative.

In the short term, the conclusion of MoUs (or equivalent) should be considered where legally binding instruments (e.g. international agreements, conventions, treaties) cannot quickly be concluded or considered a viable option.

The use of legal instruments in the matter of criminal cooperation (e.g. 2003 MLAT) could be considered where there is a serious breach of the GDPR that amounts to a criminal offence.

Finally, closer cooperation with the EU Commission during the negotiation of trade agreements could be useful in creating effective mechanisms to enforce SAs' investigative and corrective powers abroad.

ANNEX 1 - QUESTIONNAIRE

QUESTIONNAIRE – Information on the legal mechanisms that could help the enforcement of the GDPR against a controller/processor established in the United States of America (US), United Kingdom (UK) or China, who falls under its article 3(2).

This questionnaire encompasses a broad range of issues in the difficult matter of enforcing the GDPR against controller/processor established in the US, UK or China but falling under its Article 3(2), and is consecutively divided into 6 parts:

- 1° Enforcement of SA's Investigating and Corrective Powers against a controller/processor established in the US, UK or China;
- 2° Identification of legal instruments supporting the enforcement of the GDPR against a controller/processor established in the US, UK or China;
- 3° Sharing of experience about enforcing the GDPR against a controller/processor established outside the EEA;
- 4° International cooperation regarding the enforcement of the GDPR against a controller/processor established outside the EEA;
- 5° The impact of the autonomy of will on the enforcement of the GDPR outside the EEA;
- 6° Specific questions regarding the enforcement of the GDPR against a controller/processor established outside the EEA.

Please feel free to answer only the questions you are most familiar with.

PART 1. QUESTIONS ABOUT THE ENFORCEMENT OF SAS' INVESTIGATING AND CORRECTIVE POWERS AGAINST A CONTROLLER/PROCESSOR ESTABLISHED IN THE US, UK OR CHINA WHO FALLS UNDER ARTICLE 3(2) OF THE GDPR

1. Please describe the procedure/steps you would follow when exercising your investigating powers against a controller/processor established in the US, UK or China who falls under Article 3(2) of the GDPR and the legal provisions that are applicable for each step?

1.1. If appropriate, please elaborate whether a distinction has to be made between the various investigative powers described in article 58(1) of the GDPR according to their legal nature (administrative act/decision/measure, judicial act/decision/measure, criminal act/decision/investigation, other?):

- Information request
- Data protection audits
- Notification of an alleged infringement
- Access to personal data
- Access to premises

Please use below table to provide your answers:

Type of procedure	Procedural steps in case of information request	Procedural steps in case of data protection audits	Procedural steps in case of notification of an alleged infringement	Procedural steps in case of access to personal data	Procedural steps in case of access to premises
Administrative act/decision/measure					
Judicial act/decision/measure					
Criminal act/decision/investigation					
Other					

1.2. In addition, could explain how you would deal with the issue of the language to be used and indicate the legal basis if any?

2. Could you describe the procedure/steps you would follow when exercising your corrective powers against a controller/processor established in the US, UK or China who falls under Article 3(2) of the GDPR and the legal provisions that are applicable for each step?

2.1. If appropriate, please elaborate whether a distinction has to be made between the various corrective powers described in article 58(2) of the GDPR according to their legal nature (administrative act/decision/measure, judicial act/decision/measure, criminal act/decision/investigation, other?):

- Warning of a possible infringement
- Reprimands
- Order to comply with data subjects' requests to exercise their rights
- Order to comply with the GDPR provisions
- Order to communicate a data breach to the data subject
- Data processing limitation (e.g. ban on processing)
- Order to rectify/erase/restrict processing and notification to recipients
- Withdrawal of a certification
- Administrative fine

- Suspension of data flows to a recipient in a third country or to an international organization

Please use below table to provide your answers:

Type of procedure	Procedure 1 steps in case of warning of a possible infringement	Procedure 1 steps in case of reprimand	Procedure 1 steps in case of order to comply with the GDPR provisions	Procedure 1 steps in case of order to comply with the GDPR provisions	Procedure 1 steps in case of order to comply with the GDPR provisions	Procedure 1 steps in case of order to comply with the GDPR provisions	Procedure 1 steps in case of order to comply with the GDPR provisions	Procedure 1 steps in case of order to comply with the GDPR provisions	Procedure 1 steps in case of order to comply with the GDPR provisions	Procedure 1 steps in case of order to comply with the GDPR provisions	Procedure 1 steps in case of order to comply with the GDPR provisions	Procedure 1 steps in case of order to comply with the GDPR provisions
Administrative act/decision/measure												
Judicial act/decision/measure												
Criminal act/decision/investigation												
Other												

2.2. In addition, could explain how you would deal with the issue of the language to be used and indicate the legal basis if any?

3. Please describe the appropriate safeguards provided for by your national law pursuant to GDPR Article 58(4) (including effective judicial remedy and due process) and that are pertaining when exercising your investigating and corrective powers against a controller/processor established in the US, UK or China who falls under Article 3(2) of the GDPR.

3.1. In addition, please indicate the national legal provisions that are applicable and, if possible, their text in English.

Please use below table to provide your answers:

No.	Appropriate national safeguard and brief description	Legal basis (national legal provision)	English translation
1			
2			
3			

4. Please describe the national legal provisions that are applicable in your country pursuant to GDPR Article 58(5) that allows you as a Supervisory Authority (SA) to bring infringements to the attention of the judicial authorities and to commence or engage otherwise in legal proceedings in order to enforce the GDPR. Please focus on those provisions that are pertaining when you exercise your investigating and corrective powers against a

controller/processor established in the US, UK or China who falls under Article 3(2) of the GDPR.

4.1. In other words, do you have the legal possibility to summon a controller / processor who falls under article 3(2) of the GDPR, to appear in a Court in your country or in front of your office (or in front of any other public institution or body)?

- Yes
- No
- I do not know

4.2. If positive, could you describe such national legal provisions?

In addition:

4.3. Please indicate the legal basis that could open the international jurisdiction of your country to know of a case introduced by you exercising your investigating and corrective powers against a controller/processor who falls under article 3(2) of the GDPR.

4.4. Please indicate the law that would be applied to the controller/processor who falls under article 3(2) of the GDPR (beyond the application of the GDPR rules) (and the legal reasoning for applying a foreign legislation).

5. Please describe any additional powers provided by your national law that could be pertaining when exercising your investigating and corrective powers against a controller/processor established in the US, UK or China who falls under Article 3(2) of the GDPR.

PART 2. IDENTIFICATION OF THE LEGAL INSTRUMENTS SUPPORTING THE ENFORCEMENT OF THE GDPR AGAINST A CONTROLLER/PROCESSOR ESTABLISHED IN THE US, UK OR CHINA WHO FALLS UNDER ITS ARTICLE 3(2)

- 1. Please list and describe the national, European and international legal instruments you could rely on when enforcing the GDPR against a controller/processor established in the US, UK or China who falls under its Article 3(2), in the matter of Cooperation / Assistance / Act or Decision Notification / Act or Decision Recognition / Direct or Indirect Enforcement.**

In addition:

- 1.1. Please indicate whether these legal instruments are applicable in all matters (including data protection) or are specific to data protection.
- 1.2. Please specify the nature of these legal instruments (International Agreement, Treaty, Convention, Informal Agreement, Bilateral Agreement, (including Memorandum of Understanding), etc.).
- 1.3. If possible, please provide an English version of the text.

Please use the following table to provide your answers:

No	Name of the legal instrument	Geographical coverage (national, EU, international,	Coverage (Cooperation / Assistance / Act or Decision Notification / Act or Decision Recognition / Direct or Indirect Enforcement / All)	Is this instrument data protection specific? (Yes/No/N/A)	Nature of the legal instrument (International Agreement, Treaty, Convention, Information Agreement, Bilateral Agreement, other)	Link to the agreement (in English if possible)
1						
2						
3						
4						
5						

- 1.4. Please indicate any discussion or work on the issue of the international cooperation in the field of data protection that are ongoing at the moment in your country (cooperation, mutual assistance, engagement of stakeholders, promotion of exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries).

PART 3. SHARING OF EXPERIENCE AND THOUGHTS ABOUT THE ENFORCEMENT OF THE GDPR AND THE SAs' INVESTIGATING AND CORRECTIVE POWERS AGAINST A CONTROLLER/PROCESSOR ESTABLISHED OUTSIDE THE EEA BUT WHO FALLS UNDER ARTICLE 3(2) OF THE GDPR

This part of the questionnaire aims at collecting your experience and reflections on the enforcement of the GDPR and the SAs' investigating and corrective powers against a controller/processor established outside the EEA but who falls under Article 3(2) of the GDPR.

- 1. Please describe any experience (even by another SA) or knowledge that you have in the matter of enforcing SAs' investigating and corrective powers abroad (beyond the EEA zone; meaning, directly on the territory of a third country where the controller/processor is located). Examples of such experience could include sending an auditing or investigating teams abroad etc.**

- 1.1. If possible, please provide a brief account of the case(s) (facts, legal reasoning and results) and a copy of the decision in English.

In addition:

- 1.2. Do you have any knowledge of a country outside the EEA zone that would offer its cooperation in the field of data protection and/or would recognize your investigative or corrective powers?

- Yes
- No
- I do not know

- 1.3. If positive, could you elaborate on the legal framework of this international cooperation?

- 1.4. Could you describe the external resources and legal support at your disposal at national, European or international level, in order to help and support you when enforcing the GDPR against a controller/processor who falls under article 3(2) of the GDPR (e.g. support from Ministry of Justice or Foreign Affairs, or from any other public institution or body)?

- 1.5. What additional help or support could be useful in your view?

- 2. Have you heard of any application of the Principle of International Courtesy in the field of data protection in your country or in another country?**

- Yes
- No
- I am not familiar with this principle

- 2.1. If positive, could you elaborate on the case (facts, legal reasoning and results)?**

- 3. Please describe any experience in which you have received a request/demand of international cooperation/assistance/enforcement in the field of data protection from a foreign non-European data protection authority (located outside the EEA zone) (or from any other foreign non-European public institution or body acting in the field of data protection)?**

- 3.1. In addition, please describe the procedure and steps when enforcing a foreign decision (from outside the EEA zone) in the field of data protection in your country with the indication of the legal basis.**

- 4. In your view, what is the added value of the designation of a representative in the EEA in accordance with Art. 27 GDPR in case of enforcement? Have you ever initiated a case against such a representative (located in your country) of a controller/processor who falls under Article 3(2) of the GDPR? If positive, could you elaborate and describe the case (facts, legal reasoning and results)?**

- 5. In your view, what other types of actions could be taken in the EEA to ensure enforcement of the GDPR relating to processing taking place by controllers or processors established in third countries (e.g. order to stop collecting/processing personal data by means of a website)? Please explain why.**

PART 4. QUESTIONS ABOUT INTERNATIONAL COOPERATION AND ASSISTANCE IN THE MATTER OF ENFORCING THE GDPR AGAINST A CONTROLLER/PROCESSOR ESTABLISHED OUTSIDE THE EEA BUT WHO FALLS UNDER ITS ARTICLE 3(2)

- 1. What are the national legal provisions applicable in your country when a European SA requests your assistance or your cooperation in the field of data protection? Could you describe the procedure?**

- 2. In your view, what are the main obstacles to the international cooperation in the field of data protection?**

- 3. In your view, what are or what could be useful tools to improve the international cooperation in the field of data protection?**

- 3.1. In addition, please elaborate if you think it could be useful to formalize further the cooperation in this respect at the level of the EDPB?**

PART 5. QUESTIONS ABOUT THE POSSIBILITY FOR THE AUTONOMY OF WILL TO IMPACT THE ENFORCEMENT OF THE GDPR AGAINST A CONTROLLER/PROCESSOR ESTABLISHED IN THE US, UK OR CHINA WHO FALLS UNDER ITS ARTICLE 3(2)

This part of the questionnaire focuses on the possibility to recognize the impact of controller/processor's contractual or unilateral commitments in the matter of enforcing GDPR obligations.

1. Are you able to conclude an agreement with the controller / processor who falls under article 3(2) of the GDPR in order to choose a jurisdiction to which to submit their dispute?

- Yes
- No
- I do not know

1.1. If positive, could you elaborate on the legal reasoning?

In addition:

1.2. Can you rely on a choice of jurisdiction contained in the Binding Corporate Rules?

- Yes
- No
- I do not know

1.3. If positive, could you elaborate on the legal reasoning?

1.4. Can you rely on a choice of jurisdiction contained in a unilateral commitment from the controller/processor?

- Yes
- No
- I do not know

1.5. If positive, could you elaborate on the legal reasoning?

2. Can you conclude an agreement with the controller / processor who falls under article 3(2) of the GDPR in order to choose the applicable law to their dispute?

- Yes
- No
- I do not know

2.1. If positive, could you elaborate on the legal reasoning?

In addition:

2.2. Can you rely on a choice of applicable law contained in Binding Corporate Rules?

- Yes
- No
- I do not know

2.3. If positive, could you elaborate on the legal reasoning?

2.4. Can you rely on a choice of applicable law contained in a unilateral commitment from the controller/processor?

- Yes
- No
- I do not know

2.5. If positive, could you elaborate on the legal reasoning?

PART 6. SPECIAL QUESTIONS REGARDING THE ENFORCEMENT OF THE GDPR AGAINST A CONTROLLER/PROCESSOR ESTABLISHED OUTSIDE THE EEA BUT WHO FALLS UNDER ITS ARTICLE 3(2)

This last part of the questionnaire concerns very specific topics in the area of enforcing the GDPR against a controller/processor established outside the EEA but who falls under its article 3(2).

1. Could the courts in your country or any other national public institution or body review the acts and decisions from a foreign (non-European) data protection authority (located outside the EEA)?
 - Yes
 - No
 - I do not know

1.1. If positive, could you elaborate on the legal reasoning?

2. Could the courts in your country or any other national public institution or body enforce the acts and decisions from a foreign data protection authority (located outside the EEA)?
 - Yes
 - No
 - I do not know

2.1. If positive, could you elaborate on the legal reasoning?

3. What is the probative force attached to the acts and decisions of a foreign data protection authority (located outside the EEA) in your country? Could you elaborate on the legal reasoning and indicate the legal basis?

Thank you!

ANNEX 2 – SOURCES OF INFORMATION

I. International conventions and agreements

1. 1971 Hague Convention on the recognition and enforcement of foreign judgments in civil and commercial matters.
2. 2001 Agreement between the Government of Ireland and the Government of the Hong Kong Special Administrative Region of the People's Republic of China concerning mutual legal assistance in criminal matters (Treaty Series 2012, n° 2).
3. 2001 US and Republic of Ireland Agreement relating to mutual legal assistance in criminal matters.
4. 2003 Agreement on mutual legal assistance between the European Union and the United States of America (2003 MLAT).
5. 2005 Hague Convention on choice of court agreements.
6. 2007 Convention on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Lugano Convention).
7. 2009 Agreement between the European Union and Japan on mutual legal assistance in criminal matters.
8. 2016 Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences.
9. 2019 Hague Convention on the recognition and enforcement of foreign judgments in civil or commercial matters.

II. Council of Europe conventions

1. 1959 Convention on Mutual Assistance in Criminal Matters (ETS n° 30).
2. 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (now Treaty 108+).
3. 2001 Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows.

III. EU law and documents

Fundamental texts of the EU

1. Charter of Fundamental Rights of the European Union.
2. Treaty on the Functioning of the European Union (consolidated version).

EU directives and regulations

1. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
2. Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty.
3. Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I).
4. Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.
5. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on

the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

6. Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.
7. Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC.
8. 2021 Decision on the adequate protection of personal data by the United Kingdom (General Data Protection Regulation, GDPR).
9. 2021 Decision on the adequate protection of personal data by the United Kingdom (Law Enforcement Directive).

EDPB guidelines and other EU documents

1. Brief of the European Commission on behalf of the European Union as Amicus Curiae in support of neither party – United States of America v. Microsoft Corporation (US Court of Appeals, 2e Circuit), n° 17-2.
2. EDPB 3/2018 Guidelines on the territorial scope of the GDPR (Article 3) (version 2.1).
3. Final Report on ‘Data protection in the judiciary: the concept of courts/judicial authorities acting in their judicial capacities’, EDPS/2019/02-01, 2020.

Existing EU trade agreements:

1. EU-Singapore Free Trade Agreement, 19 October 2018.
2. EU-Vietnam FTA, 30 June 2019.
3. EU-Canada Comprehensive Economic and Trade Agreement (CETA), 21 September 2019.
4. EU-China Comprehensive Agreement on Investment, 30 December 2020.
5. EU-UK Trade and Cooperation Agreement, 30 December 2020.
6. 2016 Enhanced Partnership and Cooperation Agreement between the European Union and its Member States, of the one part, and the Republic of Kazakhstan, of the other part, 2016.

EU trade agreements under negotiation:

1. EU-Mercosur Trade Agreement.
2. EU-Mexico Trade Agreement.
3. EU-Australia Trade Agreement.
4. EU-New Zealand Trade Agreement.

IV. US law

Federal Law:

1. Revised version of the 1962 Uniform Foreign-Country Money Judgments Recognition Act
2. US Code, Title 18, Chapter 119, Section 2511(2)(j).
3. Undertaking Spam, Spyware, and Fraud Enforcement With Enforcers beyond Borders Act of 2006 (US Safe Web Act of 2006).
4. 2018 Clarifying Lawful Overseas Use of Data Act’ (Cloud Act).
5. FTC, Office of International Affairs, US Safe Web Act Information Sheet.

California law:

1. State of California, Civil Code, Division 3. Obligations. Part 4. Obligations arising from particular transactions. Title 1.81.5. California Consumer Privacy Act of 2018, § 1789.199.10.
2. California Code of Civil Procedure (CCP), Part 3. Of Special Proceedings of a Civil Nature, Title 11. Money Judgments of other jurisdictions, Chapter 2. Foreign-Country Money Judgments, §§1713-1725.
3. California Consumer Privacy Act of 2018.

V. UK law

1. Foreign Judgments (Reciprocal Enforcement) Act 1933.
2. UK Data Protection Act 2018 (DPA 2018).
3. UK GDPR.

VI. China law

1. 2021 Personal Information Protection Law (PIPL).
2. 2021 Data Security Law.

VII. Case-law

US case-law:

1. United States Court of Appeals, Yahoo! Inc. v. *La Ligue contre le racisme et l'antisémitisme et l'Union des étudiants juifs de France*, 433 F.3d 1199, 1202 (9th Cir. 2006) (en banc).
2. United States District Court, Hugo Elliot v. PubMatic Inc., Case 4:21-cv-01497-PJH (Northern District of California 2021).

CJEU case-law:

1. CJEU (Grand Chamber), 6 September 2017, C-413/14, *Intel Corp. v European Commission*.
2. CJEU (3d ch.), 3 October 2019, C-18/18, *Eva Glawischnig-Piesczek v Facebook Ireland Limited*.
3. CJEU (3d ch.), 9 July 2020, C-272/19, *VQ v Land Hessen*.
4. CJEU, 16 July 2020, C-73/19, *Belgische Staat v Movic BV, Events Belgium BV, Leisure Tickets & Activities International BV*.
5. CJEU (Grand Chamber), 15 June 2021, C-645/19, Facebook Ireland Limited, Facebook Inc., *Facebook Belgium BVBA v Gegevensbeschermingsautoriteit*.

VIII. MoU (or equivalent)

1. 2012 MoU between the Privacy Commissioner of Canada and the Federal Commissioner for Data Protection and Freedom of Information of Germany on mutual assistance in the enforcement of laws protecting personal information in the private sector.
2. 2013 MoU between the United States Federal Trade Commission and the Office of the Data Protection Commissioner of Ireland on mutual assistance in the enforcement of laws protecting personal information in the private sector.
3. 2014 MoU between the Privacy Commissioner of Canada and the Data Protection Commissioner of Ireland on mutual assistance in the enforcement of laws protecting personal information in the private sector.
4. 2014 MoU between the Privacy Commissioner of Canada and the College Bescherming Persoonsgegevens (the Netherlands) on mutual assistance in the enforcement of laws protecting personal information in the private sector.
5. 2014 MoU between the Privacy Commissioner of Canada and the National Supervisory Authority for Personal Data Processing of Romania on mutual assistance in the enforcement of

- laws protecting personal information in the private sector.
6. 2015 Cooperation Agreement between the Italian SA and the Albanian Data Protection Authority.
 7. 2015 MoU between the United States Federal Trade Commission and the Dutch Protection Authority on mutual assistance in the enforcement of laws protecting personal information in the private sector.
 8. 2019 MoU between the Information Commissioner for the United Kingdom of Great Britain & Northern Ireland and Canadian Radio-television and Telecommunications Commission for cooperation in the enforcement of laws protecting personal data.
 9. 2019 MoU between the Personal Data Protection Commission of the Republic of Singapore and the Information Commissioner for the United Kingdom for cooperation in the enforcement of laws protecting personal data.
 10. 2020 US Federal Trade Commission and UK ICO MoU on mutual assistance in the enforcement of laws protecting personal information in the private sector.
 11. 2020 MoU between the Privacy Commissioner of Canada and the Information Commissioner of the United Kingdom on mutual assistance in the enforcement of laws protecting personal information in the private sector.
 12. 2020 MoU between the Privacy Commissioner for Personal Data of Hong-Kong, China and the Information Commissioner for the United Kingdom for cooperation in protecting personal data.
 13. 2020 MoU between the Information Commissioner for the United Kingdom of Great Britain & Northern Ireland and the New Zealand Department of Internal Affairs for cooperation in the regulation of unsolicited electronic messages.
 14. 2020 MoU between the Information Commissioner and the Global Cyber Alliance.
 15. 2021 MoU between the Information Commissioner for the United Kingdom of Great Britain & Northern Ireland and the Office of the Privacy Commissioner for New Zealand for cooperation in the enforcement of laws protecting personal data.
 16. 2021 MoU between the Information Commissioner for the United Kingdom of Great Britain & Northern Ireland and the National Privacy Commission of the Philippines for cooperation in the regulation of laws protecting personal data.

IX. OECD documents

1. 2007 Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy.
2. 2012 Background Note on Improving International Co-operation in Cartel Investigation, DAF/COMP/GF(2012)6).
3. 2020 Summary of Discussion ‘Roundtable on Legislative Initiatives to Improve Cross-border Enforcement Cooperation’, DSTI/CP(2019)21/FINAL.

X. Other international documents

1. International Conference of Data Protection and Privacy Commissioners (ICDPPC), Global Cross-border Enforcement Cooperation Agreement, version 17, 2017.
2. Global Privacy Enforcement Network (GPEN), Action Plan for the Global Privacy Enforcement Network, 2013.
3. APEC, Cross-border Privacy Enforcement Arrangement (CPEA) (2019 version).

XI. Legal literature

Papers:

1. Azzi, A., ‘The challenges faced by the extraterritorial scope of the General Data Protection Regulation’, *Journal of Intellectual Property, Information Technology and e-Commerce Law*, Vol. 9, No. 2, 2018, p. 59.

2. Browne, O. and Watret, T., *Enforcement of foreign judgments*, 10th ed., London, Law Business Research, Lexology, 2020.
3. Cassart, A., ‘Premières réflexions sur le Cloud act: contexte, mécanismes et articulations avec le RGPD’, Bruxelles, Larcier, *Revue du droit des technologies de l’information*, Vol. 73, 2018.
4. Chivvis, M., ‘Reexamining the Yahoo! litigations: toward an effects test for determining international cyberspace jurisdiction’, *University of San Francisco Law Review*, 2007, Vol. 41, p. 699.
5. Dorwart, H., Zanfir-Fortuna, G. and Girot, Cl., ‘China’s new comprehensive data protection law: context, stated objectives, key provisions’, *Future of Privacy Forum*, 20 August 2021.
6. Elkind, D., *L’efficacité des décisions administratives étrangères dans l’Union européenne : Etude de droit administratif transnational*, Université de Bordeaux, 2018.
7. Freyria, Ch., ‘La notion de conflit de lois en droit public’, in *Travaux du Comité français de droit international privé*, 1962-1964, pp. 106-107.
8. Idot, L., “*La matière civile et commerciale*” à l’épreuve de l’intervention du Ministre de l’Economie en droit de la consommation”, note sous CJUE (1e ch.), 16 Juillet 2020, aff. C-73/19, Paris, Dalloz, *Revue critique de droit international privé*, Vol. 2, No. 15, 2021, p. 383, 394.

Books and book chapters:

1. Bradley, C.A., *International Law in the U.S. Legal System*, 3d ed., Oxford University Press, 2021.
2. Cheshire, North & Fawcett, *Private International Law*, 15th ed., Oxford University Press, 2017.
3. Folsom, R., *Principles of International Litigation and Arbitration*, 2d ed., West Academic, Concise Hornbook, 2019.
4. Greenleaf, G., *Asian Data Privacy Laws. Trade and Human Rights Perspectives*, Oxford University Press, 2017.
5. Hay, P., Borchers, P.J., Symeonides, S.C. and Whytock, Chr. A., *Conflict of Laws*, 6th ed., West Academic, Hornbook Series, 2018.
6. Millard, Chr. and Kamarinou, D., ‘Article 27. Representatives of controllers or processors not established in the Union’, in Chr. Kuner, Lee A. Bygrave and Chr. Docksey, *The EU General Data Protection Regulation (GDPR). A Commentary*, Oxford University Press, 2020, p. 597 (update of selected articles, covering developments between 1 August 2019 and 1 January 2021, May 2021).
7. Rustad, M., *Global Internet Law*, 3d ed., West Academic, Hornbook Series, 2020, pp. 182-183.
8. Spillenger, Cl., *Principles of Conflict of Laws*, 3d ed., West Academic, Hornbook Series, 2020.

ANNEX 3 - ACRONYMS AND ABBREVIATIONS

The table provides a preliminary list of acronyms and abbreviations used throughout this Study.

Acronyms and Abbreviations	Meaning
APEC	Asia-Pacific Economic Cooperation
BCR	Binding Corporate Rules
BG	Bulgaria
Charter	Charter of Fundamental Rights of the European Union
CAC	Cyberspace Administration of China
CiPL	Chinese Civil Procedure Law
CJEU	Court of Justice of the European Union
CNIL	<i>Commission nationale de l'informatique et des libertés</i>
CZ	Czechia
DE	Germany
DPA	Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information
DPA 2018	UK Data Protection Act
DK	Denmark
ECHR	European Convention on Human Rights
EE	Estonia
EEA	European Economic Area
EEA representative	Controller/processor's representative in the EEA or the EU
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
ES	Spain
EU	European Union
FI	Finland
FR	France
FTC	US Federal Trade Commission
GPA	Global Privacy Assembly
GPEN	Global Privacy Enforcement Network
GDPR	General Data Protection Regulation
HR	Croatia
HU	Hungary
ICDPPC	International Conference of Data Protection and Privacy Commissioners
ICO	Information Commissioner's Office or the UK Data Protection Commissioner
IS	Iceland
IT	Italy
LED	Law Enforcement Directive
LT	Lithuania
LU	Luxembourg
MLAT	Mutual Legal Assistance Treaty
MoU	Memorandum of Understanding
OECD	Organisation for Economic Co-operation and Development
PDPA	Bulgarian Personal Data Protection Act
PIPL	Chinese Personal Information Protection Law
PL	Poland
SA	Supervisory Authority
SDPI	Lithuanian State Data Protection Inspectorate
SE	Sweden
SI	Slovenia

Acronyms and Abbreviations	Meaning
SK	Slovakia
TFEU	Treaty on the Functioning of the European Union
UK	United Kingdom
UK GDPR	UK General Data Protection Regulation
UK	United Kingdom
US	United States of America



EUROPEAN DATA PROTECTION SUPERVISOR



Call for Expressions of Interest
2022/S 070-181896

corrigendum

(Supplement to the Official Journal of the European Union, 21.2.2022, 2022/S 036-091761)

**“Establishment of a List of Individual Experts for the implementation of the
EDPB’s Support Pool of Experts”**

TECHNICAL DESCRIPTION

CONTENTS

TECHNICAL DESCRIPTION	3
1. INTRODUCTION	3
2. TASKS AND ACTIVITIES OF THE EXPERTS	4
3. FIELDS OF EXPERTISE SOUGHT	5
4. EXCLUSION CRITERIA.....	6
5. ELIGIBILITY CRITERIA	8
6. SELECTION CRITERIA.....	9
7. DURATION OF THE LIST OF EXPERTS.....	9
8. OWNERSHIP AND USE OF RESULTS.....	9
9. ESTIMATED BUDGET	9
10. DATA PROTECTION	10
11 GENERAL	10

TECHNICAL DESCRIPTION

1. INTRODUCTION

The European Data Protection Board (EDPB) is an independent European body, which contributes to the consistent application of data protection rules throughout the European Union, and promotes cooperation between the EU's data protection authorities.

It is established by Regulation 2016/679 (General Data Protection Regulation or GDPR). The EDPB's tasks are listed in article 70 of GDPR and they include among others:

- providing general guidance to clarify the law and to promote a common understanding or EU data protection laws;
- issuing opinions to ensure consistency of the activities of national Supervisory Authorities on cross border matters (Art. 64 GDPR).
- adopting binding decisions addressed to the national Supervisory Authorities and aiming to settle disputes arising between them when they cooperate to enforce the GDPR, with the purpose of ensuring the correct and consistent application of the GDPR in individual cases;
- promoting and supporting the cooperation among national Supervisory Authorities.

The EDPB has a permanent secretariat whose missions are laid down in article 75 of GDPR and include providing analytical, administrative and logistical support to the Board.

The EDPB 2021-2023 strategy has identified the **need for improved collaboration** between authorities. In particular, pillar 2 of the strategy (supporting effective enforcement and efficient cooperation between national supervisory authorities) calls for the establishment of a **Support Pool of Experts (SPE)**, with a view of providing material support in the form of expertise that is useful for investigations and enforcement activities and to enhance the cooperation and solidarity between all SAs. Its Terms of Reference¹ were adopted on 15 December 2020.

The SPE involves both the EDPB and external experts.

In December 2021, the EDPB further identified topics and areas of expertise for which the SPE could be used. This includes and is not limited to support in the context of a specific investigative procedure, methodological tools for inspections (and capacity building), as well as elaborating documentation on national case law. In the context of the establishment of the SPE, EDPB is looking for experts with a high level of expertise and professional experience.

¹ https://edpb.europa.eu/sites/default/files/files/file1/edpb_document_supportpoolofexpertstor_en.pdf

The objective of this call for expressions of interest is to set up a list, containing sub-lists as specified in point 3 below, of external experts for the implementation of the EDPB's Support Pool of Experts, for the period 2022-2024.

2. TASKS AND ACTIVITIES OF THE EXPERTS

The subject matter experts could be expected to perform any tasks in the area of enforcement support and coordination, including one or more of the following:

- Support / participate in investigation activities (as approved and authorised by SAs, under the direction and management of national authorities, and in compliance with applicable laws) – e.g. scoping, evidence gathering and analysis, participating in a remote or onsite inspection, digital forensics / analysing data in a lawful manner and for use in regulatory procedures and/or court proceedings.
- Provide advisory services for the development and documentation of investigatory support tools and methods (in particular in technical fields) or for the purchase and use of specialist technical equipment, in order to ensure that regulatory procedures can be carried out in as effective and efficient manner as possible.
- Provide legal advisory services on the use of specific forensic methods to gather evidential quality that can be relied on in the course of a regulatory procedure and/or in court proceedings.
- Produce (written and oral) high-quality, clear, concise, and when required sufficiently detailed contributions, according to their expertise in the project selected. This may cover both technical and methodological contributions as well as non-technical/summative contributions.
- Participate in any face-to-face meetings and teleconferences organised, including as appropriate in working groups.

It should be noted that the subject matter experts are appointed “ad personam” and will not be considered as representatives of their organization or affiliation they are employed with.

For this reason, the successful applicant will be required to complete a ‘Legal Entity’ identification form (LE) in their own name, as a ‘natural person’ and not in the name of their employer. If the applicant has a 100% owned private company, then this may exceptionally be used to complete the LE form.

3. FIELDS OF EXPERTISE SOUGHT

EDPB will from time to time need to involve external subject matter experts to participate in and provide their expertise for various projects in the field of enforcement support and coordination; the range of activities is determined in line with needs of EDPB.

This call seeks natural persons/external experts to assist the EDPB in a personal capacity.

The EDPB welcomes expressions of interest from experts in many sectors, i.e. academia, research, industry, EU institutions, etc. with a relevant expertise in one or several of the following fields (each item below being a “sub-list”):

A. Technical expertise in new technologies and information security (including but not limited to the following):

1. IT auditing, information security auditing.
2. Website security, Mobile OS, internet of things, mobile application.
3. Digital forensics, Eavesdropping techniques, MITM proxy.
4. Cloud computing architectures, cloud computing models, cloud infrastructures, cloud services, cloud trust and security.
5. Behavioural advertising, digital tracking, cookies, fingerprinting, RTB and internet advertising (programmatic advertising, ad exchanges, demand side platforms, SSP, data brokers, consent management platforms), ePrivacy.
6. Anonymisation and pseudonymisation techniques; Risk analysis and attacks with respect to data re-identification (including inference attacks); Privacy enhancing technologies.
7. Cryptology; (a)symmetric cryptography; Hash functions, digital signature, message authentication; Cryptanalysis methodologies, techniques and tools; Crypto material management Key management, PKI; Homomorphic encryption; Mathematical foundations of cryptography.
8. Digital identity management and Trust Services (including security of electronic identification schemes, authentication, digital signatures); eIDAS; zero trust, identity federation; Age verification ; Biometrics including facial recognition.
9. Artificial intelligence.
10. UX, web design and dark patterns.

11. DPIA, personal data breaches, risk management.
12. Fintech.
13. Data science or statistical analysis in this field.
14. Experience in conducting exercises / training in the above.

B. Legal expertise in new technologies (including but not limited to the following):

- 1- Policy monitoring.
- 2- Digital laws, EU legal framework on data protection and privacy, legislation on forensics.
- 3- Digital ethics.
- 4- Statistical analysis in this field of activity.

4. EXCLUSION CRITERIA

Experts shall be excluded from participation if the natural person is in one of the following situations:

- a. it is bankrupt, subject to insolvency or winding-up procedures, its assets are being administered by a liquidator or by a court, it is in an arrangement with creditors, its business activities are suspended or it is in any analogous situation arising from a similar procedure provided for under Union or national law;
- b. it has been established by a final judgement or a final administrative decision that the person is in breach of its obligations relating to the payment of taxes or social security contributions in accordance with the applicable law;
- c. it has been established by a final judgment or a final administrative decision that the person is guilty of grave professional misconduct by having violated applicable laws or regulations or ethical standards of the profession to which the person belongs, or by having engaged in any wrongful conduct which has an impact on its professional credibility where such conduct denotes wrongful intent or gross negligence, including, in particular, any of the following:
 - i. fraudulently or negligently misrepresenting information required for the verification of the absence of grounds for exclusion or the fulfilment of eligibility or selection criteria or in the performance of a contract or an agreement;
 - ii. entering into agreement with other persons or entities with the aim of distorting competition;

- iii. violating intellectual property rights;
 - iv. attempting to influence the decision-making process of the contracting authority during the award procedure;
 - v. attempting to obtain confidential information that may confer upon it undue advantages in the award procedure;
- d. it has been established by a final judgment that the person is guilty of any of the following:
- i. fraud, within the meaning of Article 3 of Directive (EU) 2017/1371 and Article 1 of the Convention on the protection of the European Communities' financial interests , drawn up by the Council Act of 26 July 1995;
 - ii. corruption, as defined in Article 4(2) of Directive (EU) 2017/1371 or active corruption within the meaning of Article 3 of the Convention on the fight against corruption involving officials of the European Communities or officials of Member States of the European Union, drawn up by the Council Act of 26 May 1997, or conduct referred to in Article 2(1) of Council Framework Decision 2003/568/JHA, or corruption as defined in other applicable laws;
 - iii. conduct related to a criminal organisation, as referred to in Article 2 of Council Framework Decision 2008/841/JHA;
 - iv. money laundering or terrorist financing, within the meaning of Article 1(3), (4) and (5) of Directive (EU) 2015/849 of the European Parliament and of the Council;
 - v. terrorist offences or offences related to terrorist activities as well as of inciting, aiding, abetting or attempting to commit such offences as defined in Articles 3, 14 and Title III of Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism;
 - vi. child labour or other offences concerning trafficking in human beings as referred to in Article 2 of Directive 2011/36/EU of the European Parliament and of the Council;
- e. it has shown significant deficiencies in complying with the main obligations in the performance of a contract or an agreement financed by the Union's budget, which has led to its early termination or to the application of liquidated damages or other contractual penalties, or which has been discovered following checks, audits or investigations by a contracting authority, the European Anti-Fraud Office (OLAF) or the Court of Auditors;
- f. it has been established by a final judgment or final administrative decision that the economic operator has committed an irregularity within the meaning of Article 1(2) of Council Regulation (EC, Euratom) No 2988/95;
- g. it has been established by a final judgment or final administrative decision that the person has created an entity in a different jurisdiction with the intent to circumvent fiscal, social or any other legal obligations in the jurisdiction of its registered office, central administration or principal place of business.

5. ELIGIBILITY CRITERIA

Based on the self-declared application forms received, only candidates who meet the following minimum criteria will automatically be considered to be included in the list of external experts dependent on endorsement by an evaluation committee:

- Have fully completed their application form;
- Have experience in using English as a working language;
- Have a university degree in a relevant area, preferably at post-graduate level
- Have a minimum of three years of relevant professional experience,
- Have minimum 12 months of experience in the selected fields of expertise during the last 5 years;
- Have provided a self-assessment of their competence in the selected sub-fields
- Have provided a CV preferably in Europass format. The template (preferably in English) can be downloaded from the following web link: <https://europass.cedefop.europa.eu> and which highlights the years of experience the applicant has in the specified fields.

Exceptionally, candidates who are close to the minimum requirements for years of experience or who have a unique skillset, may be considered for evaluation and inclusion in the List.

*Only candidates whose nationality and bank accounts meet the requirements stemming from Article 176 of the Financial Regulation (Regulation 2018/1046 of the European Parliament and of the Council of 18 July 2018) can be awarded a contract.
(i.e. Are a national of, or working for a legal entity of one of the Member States of the EU or EEA; have a bank account in an EU Member State or EEA).*

6. SELECTION CRITERIA

Applicants will be evaluated according to their technical and professional capacity to meet the requirements of the Field(s) for which they are applying, following the criteria below:

- Relevance of their current job responsibilities and expertise to each of the 'Fields' applying for.
- Professional certifications held and publications will be taken into consideration.
- Their experience based on previous participation in similar projects; in particular, participation in relevant EU projects with Supervisory Authorities will be considered an advantage.

More specifically, an applicant may provide the following documentation/information:

- **A list of projects or publications** related to their declared field(s) of interest in the past 3 years. Without evidence of recent activity then it will be difficult to judge the applicant's suitability and level of experience.
- **Professional certifications** and references (e.g. links) to **publications**.

7. DURATION OF THE LIST OF EXPERTS

The CEI List of Experts compiled as a result of this procedure will be **valid for two years from dispatch of this notice and may be extended for two more years**.

Interested parties may submit an expression of interest at any time prior to the last three months of validity of the list.

New applications will be evaluated on a regular basis in order to update the List with successful applicants.

8. OWNERSHIP AND USE OF RESULTS

The results produced (including copyright and other intellectual or industrial property rights) will belong to the contracting authority. The rights will be obtained for the full term of intellectual property protection, from the moment the results are delivered and approved. Delivery and approval are considered to constitute an effective assignment of rights. This transfer of rights is free of charge.

9. ESTIMATED BUDGET

Each selected Expert will be remunerated with a fixed fee of €450 per person-day plus any travel and subsistence related costs, which will be based on EDPS's applicable rules.

A successful applicant who is added to the CEI List may be invited to participate in one or more projects. The threshold of the directive on public procurement (2014/24/EU) applies to the total of all payments to be made to each expert throughout the duration of this list of experts. If an expert has concluded contracts for a total amount exceeding €15 000 in a calendar year, the name, the locality (region of origin), amount, and subject of the contracts shall be published on the website of the contracting authority no later than 30 June of the year following contract award. The information shall be removed two years after the year of contract award.

10. DATA PROTECTION

Details on the processing of personal data associated to this procedure² are available at https://edpb.europa.eu/edpb-specific-privacy-statements_en

11. GENERAL

It is clarified that EDPB is not limited to only appointing experts registered in this database. It may select in a transparent manner any individual expert with the appropriate skills not included in the database, if deemed appropriate and in duly justified cases.

Please note that for any particular project, EDPB has the possibility under the regulations governing Calls for Expressions of Interest to conduct a simplified tender procedure whereby all Experts already placed on the List of Experts for a particular field, will be invited to provide a tailored offer for the project.

The offers received will then be evaluated on the basis of relevance and experience for the specific project, with the best submission evaluated being awarded the contract.

It is also noted that applicants that do not wish to or cannot be remunerated due to their primary employment contracts, are also eligible to apply for inclusion in the List of Experts, indicating this in the respective field of the CEI Application form.

These applicants will still be entitled to reimbursement of any travel and subsistence costs incurred from their participation in a project, should they wish to be reimbursed.

Expressions of interest should be submitted in one of the official languages of the European Union by electronic means at the following address:
<https://ec.europa.eu/eusurvey/runner/PoolOfExperts>

In case of question please contact edpb@edpb.europa.eu by adding [SPE CEI] in the subject of the email.

² If personal data is processed by the expert, this must be done in accordance with the written instructions of the data controller. Appropriate technical and organisational security measures are in place to address data processing risks (preventing unauthorised access, reading, copying, alteration or deletion of personal data, etc.).



The Contracting authority shall acknowledge receipt of the expression of interest (directly in the web interface at the end of the registration process) and shall proceed to the registration of the expert on the list (sub-list(s)) as soon as possible (and in any case within 3 months) after the date of the reception of the expression of interest as above.

Inclusion on the list (sub-list(s)) entails no obligation on the part of the contracting authority concerning the conclusion of contracts.

Contracting authority

European Data Protection Supervisor (EDPS) acting for the European Data Protection Board (EDPB)
Rue Wiertz 60,
B-1047 Brussels

Corrigendum to EDPB Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms - Editorial corrections

Item	Correction
Paragraph 49	[...] Further questions were related to the interpretation of Article 9 GDPR ⁴¹ and Article 6(1) GDPR (letters b, d, e, f) ⁴² .
Paragraph 60	[...] This is particularly important if the controller narrows down the data subject's range of choices (e.g. by not providing a Free Alternative Without Behavioural Advertising, as described below in Section 4.2.1.1) or makes choices which may risk unduly influencing the data subject's choice (e.g. by charging a fee that is such to effectively inhibit data subjects from making a free choice).
Footnote 14	[...] <i>Beschluss – der Konferenz der unabhängigen Datenschutzaufsichtsbehördendes Bundes und der Länder vom, 22 March 2023</i>
Footnote 24	Under Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (hereinafter, 'DSA'), Article 33(1), Section 5 applies to VLOPs are 'online platforms which have provide their services to a number of average monthly active recipients of the service in the Union equal to or higher than 45 million" and which are designated" as VLOPs by the European Commission under Article 33(4) DSA. According to Article 3(i) DSA, an online platform is a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public.
Footnote 50	Request, Section II ('Background and reasoning of this request'), B. The relation between consent and 'consent or pay' models, p. 3 referring to CJEU Bundeskartellamt judgment, paragraph 140 150 .
Footnote 76	The same also applies to withdrawing consent, see Article 7 (2) (3) GDPR.
Footnote 131	See also Recital 28 39 , which says that purposes ' must should be ... determined at the time of collection of the data'. [...]

Coordinated Supervision Committee Report of Activities

2022-2024



Table of Contents

1. FOREWORD	3
2. THE ROLE OF THE CSC	4
2.1 CSC Mission	5
2.2 Tasks and duties	6
3. OVERVIEW	7
3.1 CSC Rules of Procedure	7
3.2 Organisation and working methods	7
3.3 Work programme	8
4. CROSS-CUTTING ACTIVITIES	10
4.1 Data subject rights	10
4.2 Interpretation and application of EU and national laws	10
4.3 Information exchange, joint audits and coordinated inspections	11
4.4 Preparing for future coordinated supervision	11
4.5 Supporting activities	12
4.5.1 <i>External dialogue</i>	12
4.5.2 <i>Reporting</i>	12
5. SPECIFIC ACTIVITIES	13
5.1 IMI	13
5.1.1 <i>Transparency obligations</i>	13
5.1.2 <i>Users' management</i>	13
5.1.3 <i>Compliance of data protection requirements in IMI</i>	14
5.2 EPPO	14
5.3 Eurojust	14
5.3.1 <i>Joint Investigation Teams</i>	14
5.3.2 <i>Counter Terrorism Register</i>	14
5.3.3 <i>Supervisory independence</i>	14
5.3.4 <i>Secure communication</i>	14
5.4 Europol	14
5.4.1 <i>Transition of supervision</i>	14
5.4.2 <i>Access guide</i>	15
5.4.3 <i>Report on minors</i>	15
5.4.4 <i>Improving cooperation on complaints</i>	15
5.4.6 <i>Information alerts</i>	15
5.5 SIS	15
5.5.1 <i>Transition of supervision</i>	15
5.5.2 <i>Access guide</i>	16
5.5.3 <i>SIS information campaign</i>	16
5.5.4 <i>Collection of statistics on data subject rights</i>	16
5.5.5 <i>SIS Article 36</i>	17
5.5.6 <i>SIS Article 40</i>	17
5.5.7 <i>Legal interpretation of provisions of the audit cycle</i>	17
5.5.8 <i>Commission Schengen evaluation</i>	17
5.5.9 <i>eu-LISA information sharing</i>	18
5.6 VIS	18

6. LOOKING AHEAD: CHALLENGES FOR 2024-2026

19

6.1 Preparation to onboard further existing and new EU-information systems	19
6.2 Enhanced internal organisation	20



1. FOREWORD

This 2022-2024 activity report summarises the work completed by the **Coordinated Supervision Committee (CSC)** from July 2022 to December 2024. During this period, it was possible to conclude some of the actions envisaged in the second CSC working programme, covering the same period, and other important coordinated activities were designed and structured or launched and are now running.

While Europol had just come under the purview of the CSC in June 2022, we also started in March 2023 to assume supervision of the upgraded Schengen Information System (SIS). This report thus shows the work carried out in relation to these two new major EU information systems, mostly on guidance addressed to individuals on the exercise of their rights. It should also be highlighted that the CSC committed to take on board the most relevant activities that were ongoing at the time of transfer of supervision bodies.

The CSC has been working hard to accommodate the large-scale European Union (EU) information technology (IT) systems that have already come under its purview and to prepare for the arrival of new systems and for the implementation of interoperability regulations.

Looking forward to the coming years, the CSC is ready to welcome more EU IT systems and EU bodies, offices or agencies within its purview. It will tackle the outstanding items in its current 2022-2024 work programme and develop our next programme of activities.

As the scope of the CSC's activities continues to grow, we will keep the organisation and operation of the committee under constant review to ensure

an effective and efficient supervision is delivered.

We will continue to assist national data protection authorities (DPAs) in their work, by providing further clarification on the interpretation of EU and national laws, stimulating the exchange of information and best practices, and providing support for joint audits and coordinated inspections. Taking advantage of its singular framework and holistic view, the CSC will ensure that the multiple data flows among systems and transversal interactions and sharing of information between EU agencies and bodies are properly monitored. To achieve that goal, the CSC will keep developing coordinated supervisory activities covering this new reality to guarantee a high level of data protection and the safeguard of fundamental rights.

Fanny Coudert

CSC Coordinator (July - December 2024)

Clara Guerra

CSC Coordinator (July 2022 - July 2024)

Sebastian Hümmeler

Deputy CSC Coordinator

Matej Sironic

Deputy CSC Coordinator



2. THE ROLE OF THE CSC

The Coordinated Supervision Committee (CSC) consists of representatives of the national data protection authorities (DPAs) of the EU-27 countries, plus Iceland, Liechtenstein, Norway and Switzerland (non-EU Members of the Schengen Area), and the European Data Protection Supervisor (EDPS).

The CSC was established in December 2019 to ensure the coordinated supervision of large-scale EU IT systems and of relevant EU bodies, offices and agencies, in accordance with Article 62 of Regulation (EU) 2018/1725¹ or with the specific EU legal act establishing the large-scale EU IT system or the EU body, office or agency. Regulation (EU) 2018/1725 provided for a single model of coordinated supervision for large-scale EU IT systems, EU bodies, offices and agencies within the framework of the European Data Protection Board (EDPB).

In March 2023, the Schengen Information System (SIS) came under the purview of the CSC making it the fifth EU IT system, body, office or agency under its supervision. This followed the entering into operation of the upgraded SIS on 7 March 2023 with enhanced data sharing and cooperation².

Currently, the EU IT systems, bodies, offices and agencies

falling within the scope of the CSC are the following:

- Internal Market Information System (IMI)
- European Union Agency for Criminal Justice Cooperation (Eurojust)
- European Union Agency for Law Enforcement Cooperation (Europol)
- The Schengen Information System (SIS)
- Visa Information System (VIS).

The CSC also provides a forum for cooperation in the context of the European Public Prosecutor Office (EPPO), the independent supranational prosecution body responsible for investigating, prosecuting and bringing to judgment crimes against the EU budget.

Further EU IT systems, bodies, offices and agencies are planned to come within the scope of the CSC in the near future. These are:

- Entry/Exit System (EES)
- The European Travel Information and Authorisation System (ETIAS)
- The European Criminal Records Information System on non-EU-nationals (ECRIS-TCN)
- European Asylum Dactyloscopy Database (EURODAC)

1. [Regulation \(EU\) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation \(EC\) No 45/2001 and Decision No 1247/2002/EC.](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1725&from=EN)

2. [https://ec.europa.eu/commission/presscorner/detail/en/ip_23_1505.](https://ec.europa.eu/commission/presscorner/detail/en/ip_23_1505)

- Customs Information System (CIS-JHA)
- Prüm II³
- Interoperability of EES, ETIAS, ECRIS-TCN, EURODAC, Prüm II⁴, SIS, and VIS.

The CSC provides a horizontal approach to data protection supervisory activities anchored on the EDPB and enables an enhanced cooperation among DPAs and the coordination of enforcement actions at European⁵ and national levels. However, the CSC enjoys an autonomous functioning and positioning, pursuant to Article 37.2 of the EDPB Rules of Procedure⁶. The CSC has adopted its own rules of procedure and working methods⁷.

The EDPB Secretariat provides the Secretariat of the CSC and assists the CSC in the performance of its tasks. The CSC Secretariat offers analytical, administrative and logistical support including preparation of positions, and organising CSC meetings and communication between its members and with other institutions and the public.

The representatives of the national DPAs⁸ may participate in the activities of the CSC concerning a specific large-scale EU IT system or EU office, body or agency, only when their respective country applies the relevant EU legal act establishing the large-scale EU IT system or the EU office, body or agency.

2.1 CSC Mission

The central mission of the CSC is to ensure the coordinated supervision by DPAs of large-scale EU IT systems and of EU bodies, offices and agencies falling under its scope, in accordance with Article 62 of Regulation (EU) 2018/1725 or with the relevant EU legal act establishing the large-scale EU IT system or the EU body, office or agency.

For the EU IT systems, bodies, offices and agencies currently falling within the scope of the CSC, the specific mission objectives are as follows:

[The Internal Market Information System \(IMI\)](#) is a secure, multilingual online tool that facilitates the exchange of information between EU/EEA and national public authorities involved in the practical implementation of EU law and helps them to fulfil their cross-border administrative cooperation obligations in multiple Single

Market policy areas, including the General Data Protection Regulation (GDPR) and road transport, amongst others.

The CSC ensures coordination in the supervision of the processing of personal data in the IMI in accordance with Article 21 of Regulation (EU) No 1024/2012 (as modified by Article 38 of Regulation (EU) No 2018/1724).

The [European Union Agency for Criminal Justice Cooperation \(Eurojust\)](#) is based in the Hague and brings together national judicial authorities from EU Member States to fight serious organised cross-border crime.

The CSC ensures coordination in the supervision of the processing of operational personal data in the context of cooperation between the national members within Eurojust in accordance with Article 42.2 of Regulation (EU) No 1727/2018.

The [European Union Agency for Law Enforcement Cooperation \(Europol\)](#) is headquartered in The Hague and is an agency of the EU with a mandate to support and strengthen the action of EU Member States' law enforcement authorities and their cooperation in preventing and combating serious crime affecting two or more EU Member States, terrorism and forms of crime which affect a common interest covered by an EU policy.

The CSC ensures coordination in the supervision of the processing of personal data transmitted to and from Europol, and in any other issues requiring national involvement or raising questions on the implementation and application of the Europol Regulation, in accordance with Article 44.2 of Regulation (EU) 2016/794, as amended by Regulation (EU) 2022/991.

The [Schengen Information System \(SIS\)](#) allows information exchange for border management and for police and judicial cooperation in criminal matters in Europe⁹. A renewed SIS became fully operational in March 2023 with new alerts capabilities, upgraded data and other enhanced functionalities.

The CSC ensures coordination in the supervision of the processing of personal data in the SIS in accordance with Article 57 of Regulation (EU) No. 2018/1861, and Article 71 of Regulation (EU) No 2018/1862.

3. Article 59.3 of [Regulation \(EU\) 2024/982 of the European Parliament and of the Council of 13 March 2024 on the automated search and exchange of data for police cooperation, and amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations \(EU\) 2018/1726, \(EU\) No 2019/817 and \(EU\) 2019/818 of the European Parliament and of the Council \(the Prüm II Regulation\)](#).

4. [Regulation \(EU\) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations \(EC\) No 767/2008, \(EU\) 2016/399, \(EU\) 2017/2226, \(EU\) 2018/1240, \(EU\) 2018/1726 and \(EU\) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA](#).

5. We refer to 'European', rather than 'EU', as the Member States of the European Free Trade Association (EFTA), namely Iceland, Liechtenstein, Norway and Switzerland, respectively apply the EU legal acts governing some of the EU IT systems covered by the CSC. As such Iceland, Liechtenstein and Norway (who are part of the [EEA Agreement](#)), participate in the CSC activities related to both the IMI and the SIS, and Switzerland participates in the CSC activities related to the SIS.

6. https://www.edpb.europa.eu/our-work-tools/our-documents/rules-procedure/rules-procedure-version-8_en.

7. https://www.edpb.europa.eu/our-work-tools/our-documents/rules-procedure/csc-rules-procedure_en.

8. https://www.edpb.europa.eu/csc/about-csc/members-coordinated-supervision-committee_en.

9. We refer to 'Europe', rather than the 'EU', as the SIS covers those EU Member States applying the Schengen acquis, plus Member States of the European Free Trade Association (EFTA), namely Iceland, Liechtenstein, Norway and Switzerland.

The [Visa Information System \(VIS\)](#) allows [Schengen States](#) to exchange visa data. It processes data and decisions relating to applications for short-stay visas to visit, or to transit through, the Schengen Area. The system can perform biometric matching, primarily of fingerprints, for identification and verification purposes. The VIS was under the scope of the Visa Information System Supervision Coordination Group (VIS SCG)¹⁰ as set up by Regulation (EC) No 767/2008 to ensure a coordinated supervision in the area of personal data protection of the VIS information system. The VIS SCG was provided by the EDPS.

Regulation (EU) 2021/1134 amends with different application dates, among others, Regulation (EC) No 767/2008 (VIS Regulation). Among its amended provisions, Article 43(3) VIS Regulation mandates that the cooperation between the supervisory authorities and the EDPS shall take place within the framework of the European Data Protection Board. As a consequence, the coordinated supervision of the VIS is now to be carried out within the European Data Protection Board and its CSC.

The CSC also provides a forum for cooperation in the context of the [European Public Prosecutor's Office \(EPPO\)](#), an independent and decentralised prosecution office of the EU with the competence to investigate, prosecute and bring to judgment crimes against the EU budget, such as fraud, corruption or serious cross-border VAT fraud.

The CSC ensures coordination in the supervision of the processing of operational personal data in the context of cooperation between the national members within the EPPO in accordance with Article 87.3 of Regulation (EU) No 1939/2017.

2.2 Tasks and duties

Within its mission to ensure the coordinated supervision of large-scale EU IT systems and of EU bodies, offices and agencies, the CSC:

- Exchanges relevant information;
- Assists the DPAs in carrying out audits and inspections;
- Examines difficulties of interpretation or application of the EU legal act establishing the large-scale EU IT system or the EU office, body or agency under the scope of the CSC;
- Studies problems with the exercise of independent supervision or with the exercise of the rights of data subjects;
- Draws up harmonised proposals for solutions to issues; and
- Promotes awareness of data protection rights.

The CSC produces a report of its activities on coordinated supervision every two years that is provided to the EDPB for submission to the European Parliament, the Council, the European Commission and other relevant parties that

are subject to its coordinated supervision.

10. https://www.edps.europa.eu/data-protection/european-it-systems/visa-information-system_en



3. OVERVIEW

3.1 CSC Rules of Procedure

The [CSC's Rules of Procedure \(RoP\)](#) were adopted at its first meeting in 2019. During 2023, there were discussions for a possible revision of the RoP, and it was agreed that no amendments were needed at that time.

3.2 Organisation and working methods

The CSC elects a Coordinator and at least one Deputy Coordinator from among its members. The term of office for both Coordinators and Deputy Coordinators is two years.

In November 2022, the CSC re-elected Clara Guerra from the Portuguese DPA as CSC Coordinator. Sebastian Hümmeler from the German Federal DPA was re-elected in November 2023 as Deputy Coordinator. In view of the increasing number of EU IT systems coming under the purview of the CSC, and in order to prepare for a growing workload, in March 2024 the CSC elected, for the first time, a second Deputy Coordinator: Matej Sironič from the Slovenian DPA.

In July 2024 the CSC elected Fanny Coudert from the EDPS as its new Coordinator for a term of two years. She will lead the work of the CSC with the support of the two existing Deputy Coordinators.

The Coordinator convenes and chairs the meetings, acts

as a contact point in CSC matters, sets the draft agenda, and carries out all the tasks that have been assigned to them in the RoP. The Deputy Coordinators support the Coordinator in performing these tasks and in the absence of the Coordinator.

The Coordinator convenes and chairs the meetings, acts as a contact point in CSC matters, sets the draft agenda, and carries out all the tasks that have been assigned to them in the RoP. The Deputy Coordinators support the Coordinator in performing these tasks and in the absence of the Coordinator.

The CSC is mandated to meet at least twice a year and normally in-person meetings take place in Brussels, though where possible or necessary, such as during the COVID-19 pandemic, meetings are organised by way of videoconference¹¹.

In the last two years, coinciding with the end of the COVID-19 pandemic, in-person meetings have resumed and, as a consequence of increased CSC activity, the number of meetings per year has doubled. To keep a necessary flexibility in the CSC's way of working and being mindful of the limited budget allocated to the EDPB, including for CSC activities, a reasonable balance between in-person and remote/hybrid meeting formats has been achieved.

In addition, in 2024, the in-person meetings have been scheduled for one and a half days to allow adequate

¹¹. In accordance, respectively, with Article 12.1 and Article 16.2 of the CSC Rules of Procedure.

discussion of all agenda items. From March 2023, meeting agendas were restructured to include data issues relating to borders, asylum and migration, after the entry into operation of the new SIS.

During the period covered by this report, from July 2022 to December 2024, twelve meetings of the CSC took place on:

- 6 July 2022 – 6th Meeting of the CSC in a hybrid format;
- 30 November 2022 – 7th Meeting of the CSC in a hybrid format;
- 22 March 2023 – 8th Meeting of the CSC in a hybrid format;
- 14 June 2023 – 9th Meeting of the CSC in an in-person format;
- 7 September 2023 – 10th Meeting of the CSC in a remote/online format;
- 29 November 2023 – 11th Meeting of the CSC in an in-person format;
- 19 - 20 March 2024 – 12th Meeting of the CSC in an in-person format;
- 29 May 2024 – 13th Meeting of the CSC in a remote/online format;
- 2-3 July 2024 – 14th Meeting of the CSC in an in-person format;
- 25 September 2024 – 15th Meeting of the CSC in a remote/online format;
- 6 November 2024 – 16th Meeting of the CSC in a remote/online format; and
- 10-11 December 2024 – 17th Meeting of the CSC in an in-person format.

Summaries of discussions at CSC meetings [can be viewed here](#).

Participation in CSC meetings can vary depending on which EU IT system, body, office or agency subject to CSC supervision, as well as the respective EU legal act, is to be discussed. In terms of the current EU IT systems, bodies and agencies supervised, participation is as follows:

- IMI: The EDPS and the national DPAs of the 27 EU Member States participate in activities in relation to IMI together with the national DPAs of Iceland, Liechtenstein, and Norway as their respective countries also apply the EU legal acts governing IMI;
- Eurojust: The EDPS and the national DPAs of the 27 EU Member States participate in activities in relation to Eurojust;
- EPPO: The EDPS and the national DPAs of the 23 EU Member States¹² that participate in activities in relation to the EPPO;
- Europol: The EDPS and the national DPAs of the 26 EU Member States that are part of Europol participate in activities in relation to Europol; and

- SIS: The EDPS and the national DPAs of the Schengen Member States (27 EU Member States with Cyprus joining the SIS in July 2023, plus Iceland, Norway, Liechtenstein and Switzerland) participate in activities in relation to SIS.
- VIS: The EDPS and the national DPAs of the Schengen Member States (27 EU Member States plus Iceland, Norway, Liechtenstein and Switzerland) participate in activities in relation to VIS.

An overview of the CSC members and their participation [can be found here](#).

3.3 Work programme

The [CSC's second work programme covering 2022-2024](#) was adopted on 6 July 2022. This ambitious programme was published just after Europol came under the CSC's purview. Within the context of the CSC, Europol joined Eurojust and the EPPO to form a trilogy of EU IT systems in a field where processing of personal data has a great impact on the rights of individuals. This reality requires constant and effective monitoring from DPAs to ensure that the level of interference with the fundamental rights to data protection and privacy, as provided for by the EU Charter of Fundamental Rights, is really necessary and proportionate to accomplish the important public interest of combatting serious and organised crime, including terrorism.

Building on previous experience of relevant supervisory bodies, the CSC has planned to intensify its supervisory activities in all EU IT systems within its remit, through coordinated targeted actions, based on enhanced cooperation and information exchange between the EDPS and the national DPAs to ensure effective results. This approach has turned out to be successful by enabling swifter verifications at national level with faster outcomes.

Over the 2022-2024 work programme period, new EU IT systems were expected to be set up, along with some components of the interoperability scheme, and existing EU IT systems were expected to be renewed with extended functions, such as the SIS and Europol information systems. The CSC therefore included in the work programme a transversal supervisory activity covering both Europol and SIS. However, delays in the implementation of the new EU IT systems (EES, ETIAS and VIS) and the consequential lack of use of the legal possibilities for new data processing meant that some of the programmed activities have been postponed.

The 2022-2024 work programme focused on data subjects' rights as a key-area of activity. The CSC planned to reinforce awareness raising and to provide more guidance to assist

¹². [Commission Decision \(EU\) 2024/807 of 29 February 2024 confirming the participation of Poland in the enhanced cooperation on the establishment of the European Public Prosecutor's Office, OJ L, 29.2.2024](#) confirmed the participation of Poland in the EPPO and entered into force on the 20th day after its publication. Therefore, Poland became the 23rd Member State participating in the EPPO. The EPPO will be operational in Poland when the European Prosecutor for Poland is appointed by the Council of the European Union. This appointment was foreseen for July 2024.

individuals in navigating the network of EU IT systems, data controllers and different rules to exercise their rights. During these two years, the CSC took important steps in this regard.

The CSC also committed to improve its dialogue with stakeholders, in particular with NGOs, academia and researchers working in this field to promote debate on issues of common interest. That goal was accomplished with a first invitation to meet with some NGOs where a fruitful exchange of information, ideas and expectations took place.

The CSC is firmly committed to ensure that all individuals can enjoy an effective European area of freedom, security and justice.

In general, the main objectives of the work programme for this period were achieved with some activities being completed, while others were launched and are ongoing. A few activities were put on hold awaiting the implementation of new EU IT systems or the application of new functionalities that imply new types of data processing.



4. CROSS-CUTTING ACTIVITIES

In line with its biannual work programme, the CSC carried out its activities during the period July 2022 - December 2024 around the following four main axis:

1. Promote and facilitate the exercise of data subject rights;
2. Examine difficulties of interpretation or application of EU and national laws;
3. Exchange information and conduct joint audits or coordinated inspections; and
4. Prepare for the coordinated supervision of EU IT systems, bodies, offices and agencies that are planned to fall under the CSC's scope.

CSC specific activities relating to the EU IT systems, bodies, offices and agencies currently falling within its scope are described in Section 5 of this report.

The CSC has also worked on other activities that are not included in the work programme but that participating DPAs have brought to its attention, based on their relevance, urgency and/or unforeseen character.

4.1 Data subject rights

One of the main legal tasks of the CSC is to consider challenges related to the exercise of data subject rights, and to promote awareness of data protection rights. In this context, the CSC worked on two different plans and

carried out activities addressed to data controllers and to data subjects.

The CSC made recommendations to data controllers on the exercise of their data protection obligations, such as the information to be provided to data subjects and how they could handle the requests submitted by data subjects when exercising their rights.

The CSC also elaborated guidance to data subjects on their data protection rights. The CSC promoted updated guides on the exercise of data subjects' rights with respect to the new upgraded SIS and the Europol information systems.

Finally, the CSC members exchanged information on best practice on data subject's rights.

4.2 Interpretation and application of EU and national laws

The CSC is a significant forum for discussion where DPAs can exchange information on national experiences, practices and legal provisions, in particular whenever there are difficulties of interpretation or application of EU and national laws. In the past two years, DPAs discussed several issues, such as supervision challenges in the field of police and judicial cooperation. Other significant topics were the applicable legal framework for Schengen data processing, in particular when data subjects' rights are at stake, and the issues emerging from simultaneous requests for access in different Member States vis-à-vis the SIS or the interpretation of Article 47 of the Europol Regulation.

The CSC has also started to discuss the full extension of the SIS obligation for DPAs to carry out an audit every four years using international auditing standards. The interpretation of this legal provision is very relevant, since similar articles are provided in other EU legal instruments.

4.3 Information exchange, joint audits and coordinated inspections

The sharing of information among DPAs on data processing at European and national levels, and especially in those areas that could present higher risks to individual rights, such as in the area of law enforcement of criminal matters, is of paramount importance. This information sharing not only improves supervisory activities at national and European levels, but also streamlines the work of the CSC when designing joint coordinated inspections.

The information provided by the EDPS with regard to various central EU IT systems, in particular prior opinions on certain data processing activities associated with new projects and inspection reports, has been of utmost relevance for national DPAs to better understand data processing operations at EU level. This information is based on the data collected and transmitted by Member States and further queried and consulted by Member States, and enables national DPAs to conduct their own national inspections in a more targeted way. This exchange has also allowed the EDPS to gather important feedback from the national DPAs on the reality of operations at the Member State level.

This exchange of information has been a basis for mutual assistance in conducting audits, including contributing to the subjects that are inspected at central EU level. This has included the participation of some national DPAs in EU-level inspection teams during the current reporting period, for example in the Europol annual inspection. This collaboration has also helped to promote best practice on the engagement of competent authorities both at EU and national levels.

Lastly, the work of the CSC in preparing the joint inspection actions has benefitted immensely from the close cooperation and assistance between the EDPS and the national DPAs, which has allowed the achievement of a more effective coordinated supervision based on a dynamic interaction between the national and the European levels and the ability to follow data flows across systems.

4.4 Preparing for future coordinated supervision

During this reporting period, two EU large-scale IT systems were brought under the scope of the CSC: the upgraded SIS entering into operation in March 2023 and the VIS.

The CSC followed closely the development of the new EU IT systems, including the components of the interoperability

structure, as well as the envisaged entry into operation of the revised EU IT systems. Despite the consecutive schedules advanced for the implementation of these new or enhanced EU IT-systems, the dates of entry into operation have been continuously postponed, in particular with respect to the EES and the ETIAS and, consequently, the upgraded VIS.

Within that context, the CSC invited the European Commission (DG HOME) to make a presentation to its members on the latest progress and their connection with the overall interoperability system and on the information campaign in preparation for the launch of the EES.

As a consequence, some of the CSC's planned activities have not been carried out yet, as they depend on progresses in the deployment of the new EU IT systems. Nevertheless, the CSC has undertaken other activities in preparation for future deployment specifically of the entry into operation of EES and ETIAS.

Since such EU IT-systems are being implemented at national level, competent authorities need advice and guidance in terms of data protection issues. Hence, the CSC considered it imperative to exchange information amongst DPAs to establish an appropriate monitoring of the situation from the outset and facilitate the provision of advice and guidance where needed.

Within this context, the EDPB representatives in the ETIAS Fundamental Rights Guidance Board (EFRGB) also provided information to CSC members on the discussions held at that level related to data protection issues.

More recently, some issues have arisen in the interpretation and application of the ETIAS Regulation related to the exercise of data subjects' rights, as well as the data controllers' obligations to carry out a data protection impact assessment and to provide information to data subjects. Frontex requested the CSC to step in and coordinate actions across these issues, in close cooperation with Frontex, to ensure the establishment of a common approach at national level. The CSC and its members also participated in data protection working groups organised by Frontex to provide support and receive relevant information.

Rapid progress on the technical and organisational implementation of the ETIAS at central and national level with open data protection issues still in place, significantly reduces the likelihood that changes may be implemented that are necessary to safeguard the fundamental right to protection of personal data and others such as the right to non-discrimination. Therefore, the CSC addressed a letter to the European Commission to inform them about the open data protection issues and highlight the urgency required to solve them.

The CSC has also been a forum for exchange of information, experiences and ideas. One of the most significant issues on the table during the reporting period was the preparation

and internal organisation of the national DPAs' work to perform their roles in the near future as the number of EU IT systems under their supervision continually increases. This is a significant challenge for the national DPAs, the EDPS and the CSC.

One of the key elements of the preparation for the new EU IT systems falling within the scope of the CSC has been organisational issues within the Committee itself. The CSC has discussed how to improve its working methods, namely the organisation of its meetings, including how they are structured with respect to different subject matters and membership rights depending on which countries participate in the supervision of which EU IT system and/or body, office or agency, and ensuring enough time is provided for adequate debate of complex issues and activities.

Another issue is the allocation of resources by DPAs to the work of the CSC that must be balanced with the fulfilment of their competing tasks at national and EU levels. This matter has been intensely discussed during the past two years. Issues highlighted include a lack of human, financial and technical resources to supervise so many information systems at national and EU levels, with the added challenges of enabling effective supervision of all the interactions between the systems and their respective data flows and data processing operations.

In particular, the CSC discussed this important matter based on the results of studies commissioned by some DPAs on supervision requirements, inspection challenges and resources requirements. In September 2023, in an informal initiative outside of the CSC, a workshop took place, promoted by the Dutch DPA, to share views and projects on these subjects. A follow-up workshop took place on 7 March 2024.

4.5 Supporting activities

A significant role for the CSC is to be a privileged platform for cooperation and mutual assistance among national DPAs and the EDPS in performing inspections, as well as to promote a closer engagement between the European and national levels. During this reporting period, national DPAs instigated numerous requests for exchange of information on specific problems identified at national level within the CSC, which fed discussions held between CSC members.

4.5.1 External dialogue

The CSC fosters dialogue and engagement with stakeholders, in particular with civil society. As such, representatives of two selected NGOs (EDRi, Access Now) joined a dedicated part of the CSC's November 2023 meeting for an initial session.

Specifically, these NGOs presented their ongoing activities and developments in CSC-related matters. The CSC members and these NGOs also exchanged on potential synergies, always respecting the CSC's obligations and

independence. The input from these NGOs at the meeting was substantial, very useful, and was seen as a successful start to widening and institutionalising substantive dialogue with stakeholders.

The opening of a dialogue with NGOs active in data protection and in contact with data subjects is important. In the law enforcement area, the number of complaints and instances of direct interaction with the DPAs is quite low, unlike for GDPR matters. Individuals, both EU citizens and third country nationals, tend to not contact DPAs in relation to police or judicial matters. Therefore, DPAs have less knowledge of possible data infringements.

Engagement with organisations who work in the field and have meaningful interventions with individuals as data subjects is a very useful source of information for the work of CSC that can help the committee better prepare and target its supervisory activities.

4.5.2 Reporting

The CSC Coordinator reports to the EDPB on the CSC activities at least twice a year, in accordance with Article 4.2 of the CSC Rules of Procedure. Therefore, every six months, the CSC Coordinator has provided an update at the EDPB plenary on the coordinated supervision actions during the previous semester. During this reporting period, five reports were presented to the EDPB at the July 2022, January 2023, July 2023, January 2024 and July 2024 EDPB plenary meetings.



5. SPECIFIC ACTIVITIES

This section describes the specific activities undertaken by the CSC during this reporting period with respect to the EU IT systems, bodies, offices or agencies currently under its supervision.

5.1 IMI

5.1.1 Transparency obligations

The CSC has worked on a set of recommendations on IMI transparency obligations for data controllers. The [final recommendation document](#) was adopted at the CSC meeting in March 2024 and published in April 2024.

The EU internal market rules give individuals and businesses the right to move freely within the European Economic Area (EEA) for work, study, or other purposes. The recommendations address data controllers within authorities that are involved in the cooperation procedures for applying these rules, via the IMI, and are required to exchange information with competent authorities in other Member States, and therefore to process personal data in a manner that complies with Regulation (EU) 2016/679, the General Data Protection Regulation (GDPR).

Under the GDPR, transparency obligations play a key role in ensuring the rights of data subjects in relation to the processing of their personal data. The CSC's recommendations are intended to assist data controllers in complying with the GDPR's data protection provisions on the information to be provided to data subjects, in relation to the data processing their competent authority carried

out when using the IMI.

The recommendations briefly describe what information must be given to data subjects, and when and how this information must be provided under the GDPR in combination with Regulation (EU) No 1024/2012 (the IMI Regulation).

The IMI Regulation determines that a competent authority using the IMI, being a data controller, should ensure that data subjects are informed as soon as possible about the processing of their personal data in the system, and of the identity and contact details of the data controller and of its representative, if any. They must also be informed of their individual rights and how they can exercise them. These information duties must be complied with in accordance with Articles 13 and 14 of the GDPR.

5.1.2 Users' management

The CSC had an initial exchange on a supervisory action on how national competent authorities exercise their obligations concerning IMI and the management of users' access to the system. The CSC has discussed the format of such a coordinated activity starting with a fact-finding exercise and then, based on the results of that exercise, the possible development of a joint guidance document and/or enforcement at national level.

5.1.3 Compliance of data protection requirements in IMI

The CSC invited representatives of the European Commission to present their initiative with IMI national contact points in Member States and relevant competent authorities to enhance compliance of data protection requirements in IMI.

5.2 EPPO

During the reporting period, the CSC has been monitoring the implementation of European Delegated Prosecutors' offices at Member States level, including specific relevant national laws and the interplay between the EPPO case management system at national level and national databases, which are respectively supervised by the EDPS and by the national DPAs.

To assess this interplay and the actual conditions under which the European Delegated Prosecutors work at national level and apply national law while inserting data in the EPPO case files, the CSC promoted a joint activity involving the EDPS and national DPAs to make operational visits to European Delegated Prosecutors' offices in each Member State, on a rotating basis.

The Portuguese DPA volunteered to participate in this activity, together with the EDPS. For that purpose, a working arrangement was signed in December 2022. In 2023, the Portuguese DPA and the EDPS, each acting within their own competence, examined the integration of systems and relations between EPPO case files, the EPPO case system, and the national source databases at the local European Delegated Prosecutors' office. This joint visit with the EDPS at national level was the first of its kind and will serve as a pilot for future coordinated activities.

5.3 Eurojust

5.3.1 Joint Investigation Teams

The CSC has surveyed the participation of third country authorities in Joint Investigation Teams (JIT) supported within the scope of Eurojust, in view of the lack of data protection clauses in JIT agreements. The CSC survey found that in the great majority of the cases, the third country involved either held an adequacy decision or had signed a cooperation agreement with Eurojust and/or Europol. Following an exchange with Eurojust, the CSC was informed that Eurojust is drafting a model clause to insert in the JIT agreement. The CSC will continue to monitor the situation at national level.

5.3.2 Counter Terrorism Register

The CSC has taken up the subject of data quality issues related to data inserted in the Eurojust Counter-Terrorism Register (CTR).

A drafting team set up in 2023 prepared a questionnaire to facilitate fact-finding at national level on the reasons why the personal data processed in the CTR is not kept up to date. The outdated information in the CTR, available to all Member States, could represent a major negative impact on a data subjects' rights and freedoms. This coordinated action was launched at the end of May 2024.

5.3.3 Supervisory independence

The CSC has also started to gather information from its members on their assessment, based on relevant national law provisions, regarding the DPAs' independence, powers and legal tasks in relation to police and judicial cooperation in criminal matters. The specific focus of the investigation is to assess any impact on the supervision of Eurojust (and Europol) at national level.

5.3.4 Secure communication

Over the past two years, an activity related to the issue of secure communication channels for exchanges between Member States and Eurojust has been ongoing. For a couple of Member States, the situation was improved after the intervention of national DPAs, but was finally concluded at central level, following recommendations by the EDPS.

5.4 Europol

5.4.1 Transition of supervision

The CSC has ensured the smooth transition of supervision from the Europol Cooperation Board (ECB). This has included the transfer of ongoing activities and assessing new possibilities for cooperation and exchange of information between DPAs and law enforcement authorities.

This work has included following closely the implementation from June 2022 of the new legal framework that followed the amendments to Regulation (EU) 2016/794 (the Europol Regulation)¹³. In particular, the CSC has focused on the determination of the purposes of data processing by the national competent authorities and by Europol. The CSC is looking to address the so-called 'big data challenge' in close cooperation with the EDPS and national DPAs, either by checking compliance with national law when data is transmitted to Europol or compliance with the Europol Regulation when data is further processed by

¹³ Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation.

Europol. Special attention has been given to processing of data without data subject categorisation.

5.4.2 Access guide

In July 2023, the CSC published '[Europol's information systems - a guide for exercising data subjects' rights: the right of access, rectification, erasure and restriction](#)'. The content of the Guide was provided by Member States and compiled by the CSC.

Individuals whose personal data are collected, held or otherwise processed by Europol are entitled to rights regarding their personal data, namely the right of access, rights to rectification, erasure or restriction of the data, and the right to have the legality of transfer of their personal data verified by a national DPA or, where applicable, by the EDPS. The CSC guide describes how those rights can be exercised.

The guide is divided into three sections: a description of the data categories and exchange of personal data between Member States and Europol; a summary of the rights granted to individuals whose personal data are processed in Europol's IT systems; and a description of the procedure for exercising the right of access in each of the countries concerned.

The Guide also lists contact points for the relevant body to which requests for access, rectification and/or erasure should be addressed in each Member State, together with the contact details of the national DPAs and of the EDPS. Finally, as annexes, model letters are provided that can be used to file requests to the relevant national competent authority where that authority does not require a specific standard form.

5.4.3 Report on minors

Following the 2022 Audit Report of the EDPS on Europol's processing of personal data of minors under 15 years old provided to Europol by third countries and international organisations¹⁴, in 2023 the CSC undertook a coordinated activity on Europol with respect to the transmission by Member States of data on minors as suspects. Almost all concerned national DPAs conducted verifications at the national level to assess the lawfulness of such data transmission to Europol and provided feedback to the CSC.

The CSC is currently collecting the key-findings to draft a joint report on the exercise.

5.4.4 Improving cooperation on complaints

The CSC has set up an activity to determine internal procedures (including data flows, deadlines, interpretation of the extent of checks, and identification of scenarios) for cooperation between the EDPS and national DPAs to handle complaints under Article 47 of the Europol Regulation.

The main aim of the activity is to enhance cooperation between EDPS and national DPAs, make the complaints process more efficient and shorten as much as possible the deadlines to reply to data subjects. Most of the complaints received are connected to the exercise of data subjects' rights.

A brief guidance note for cooperation on the implementation of Article 47 complaints, including specific steps, procedures and deadlines, is being developed.

5.4.5 Information alerts

The CSC is monitoring the implementation of the provisions on 'information alerts' inserted in the new SIS by Member States, either at EU level (Europol) or national level (SIS). This includes checking that the periodic reporting mechanism is in place. This will be the first cross-system supervisory activity within the scope of the CSC activities.

However, the criteria for information alerts relating to the SIS Regulation were still to be established by the Europol Management Board, so this CSC activity has not yet been launched.

5.5 SIS

5.5.1 Transition of supervision

During this reporting period, the upgraded SIS, which came into operation in March 2023, was brought under the scope of CSC.

The transition of coordinated supervision from the SIS II Supervision Coordination Group (SCG)¹⁵ to the CSC was successful and seamless. The SIS II SCG itself had taken over from the Schengen Joint Supervisory Authority (JSA)¹⁶ when the second-generation SIS (SIS II) entered into force on 9 June 2013.

The CSC decided to take stock of the most relevant ongoing activities of the SIS II SCG, such as the coordinated inspections on the alerts regarding discreet and specific checks under Article 36 of the SIS II Decision and the updated Guide for the exercise of data subjects' rights.

14. https://www.edps.europa.eu/data-protection/our-work/publications/audits/2023-09-06-audit-report-europol_en.

15. https://www.edps.europa.eu/data-protection/european-it-systems/schengen-information-system_en.

16. https://www.edps.europa.eu/data-protection/our-work/publications/scg-documents/archived-webpage-former-schengen-joint_en.

The SIS has a special legal regime¹⁷ with respect to reporting that requires annual reporting of coordinating activities, rather than biannual reporting as is the norm for other EU IT systems, bodies offices or agencies under the scope of the CSC.

2023 is the first (partial) year that SIS has been under the scope of CSC and coincides with the biannual reporting of CSC activities. Therefore, the 2023 and 2024 CSC Reports on SIS Coordinated Activities are included as part of this document.

The annual assessment of SIS statistics provided by Member States on data subject rights (see 5.5.4 below) is a new reporting activity and should be considered as a stand-alone document. This document/report is being finalised at the time of publication of this report.

Next year CSC will produce a report dedicated to CSC coordinated activities in 2025 with respect to SIS and an assessment of 2024 SIS statistics.

5.5.2 Access guide

In April 2023, the CSC published '[The Schengen Information System - a guide for exercising data subjects' rights: the right of access, rectification and erasure](#)'. This guide had been compiled by the SIS II SCG. It was then reviewed and adopted by the CSC.

Within the SIS, any individual is guaranteed the right of access to their own data, the right to rectification of inaccurate data and the right to the erasure of unlawfully stored data.

The 2023 guide outlines those rights and describes how they can be exercised. It takes into account the recent changes brought by the current SIS legal framework and the revision of the EU data protection framework, as the SIS Regulations now refer to the exercise of some rights as laid down under Regulation (EU) 2016/679 - the General Data Protection Regulation (GDPR)¹⁸, and Directive (EU) 2016/680 - the Law Enforcement Directive (LED)¹⁹.

The guide has three sections: a description of the SIS; a description of the rights granted to the individuals whose

data are processed within the SIS; and a description of the procedure for exercising these rights in each of the Schengen State countries concerned, together with contact details for the competent national authorities.

Annexes to the guide give three model letters to be used by applicants to request access, and to rectify or erase their personal data in cases where the national competent authority does not require a specific standard form.

5.5.3 SIS information campaign

The CSC engaged strongly with the European Commission for the information campaign around the new SIS, in particular in coordinating implementation at national level. A link to the CSC website for the Guide for exercising the right of access was included in the Commission's digital leaflet²⁰ and general presentation²¹ on the renewed SIS.

5.5.4 Collection of statistics on data subject rights

As previewed under 5.5.1 above, the CSC is tasked with developing and drafting an annual report from information provided by Member States to submit to the EDPB on the exercise of data subjects' rights, on court proceedings, and on mutual recognition of final decisions. This assessment is to be included in the joint report of activities regarding the SIS pursuant to Article 54.3 of Regulation (EU) 2018/1861 and Article 68.3 of Regulation (EU) 2018/1862.

The format of the template for use by Member States to report on data subject rights related to the SIS regulations is set out in Commission Implementing Decision (EU) 2022/2206²².

2023 is the first year for which CSC will publish a report on these SIS statistics.

In 2023, the CSC adopted a model letter for national DPAs to send to Member State competent authorities for SIS to raise awareness on the new obligation to collect statistics on data subjects' rights. The letter includes information on the obligations and court proceedings, the template laid down by the Commission's Implementing Decision indicating the statistics to be provided and details of where to transmit the statistics collected (i.e., the CSC

17. Obligations under Article 54.3 of [Regulation \(EU\) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System \(SIS\) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation \(EC\) No 1987/2006 and Article 68.3 of Regulation \(EU\) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System \(SIS\) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation \(EC\) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU](#).

18. [Regulation \(EU\) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC \(General Data Protection Regulation\)](#).

19. [Directive \(EU\) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA](#).

20. [The Schengen Information System guaranteeing freedom, security and justice \(Guide\)](#).

21. [The Schengen Information System guaranteeing freedom, security and justice \(Presentation\)](#).

22. [Commission Implementing Decision \(EU\) 2022/2206 of 11 November 2022 laying down the reporting template for the annual reports to the European Data Protection Board by Member States on the exercise of the rights of data subjects related to the Schengen Information System](#).

Secretariat).

5.5.5 SIS Article 36

During 2019, the SIS II Supervision Coordination Group (SCG) was informed of reports of an increase in Article 36²³ alerts in the SIS. These alerts relate to discreet surveillance, which are generated and used without the knowledge of the individual concerned.

This increase was confirmed, and the SCG agreed to conduct a coordinated activity, which would involve a short questionnaire and onsite checks. The purpose of this exercise would be twofold: to gather more specific information and statistics about the use of Article 36 alerts by competent authorities; and to enable the national DPAs to assess the legality and the conditions under which such alerts are inserted and maintained in SIS II.

A short questionnaire was developed by the SCG to gather specific information and statistics about the use of Article 36 alerts by Member States. A checklist for national DPAs to use during onsite inspections was also developed.

However, with the advent of the COVID-19 pandemic in 2020 few DPAs were able to conduct inspections before they stopped for almost two years. In 2022 and 2023 the DPAs resumed this activity.

This work, initiated under the SCG, was transferred to the CSC. The CSC members have reported on their supervision actions and the findings have been assessed by CSC. A report was published in October 2024²⁴ drawing conclusions on the level of compliance, identifying any issues, and providing a set of recommendations with regard to the documentation of the alerts, their quality, the time limits and retention period, as well as substantive and technical issues.

5.5.6 SIS Article 40

SIS Article 40²⁵ alerts enable Member States to enter data, such as partial fingerprints, on unknown wanted persons. Such alerts should only be entered into SIS when there is a very high probability that they belong to the perpetrator of a terrorist act or other serious crime. From the outset of its supervision, the CSC has monitored the statistics on these alerts since this is a new alert in the SIS within the new capabilities of the system.

In the first three months of operation, only 14 alerts by two Member States were introduced to the system. The concerned Member States were advised in case they

wished to verify the alerts or check for further information.

The CSC members also exchanged information related to the interpretation of Article 40 and on the existence of national provisions or internal policies establishing criteria or providing guidance to ascertain the requirement of very high probability that the latent fingerprint belongs to a perpetrator.

The CSC continues to monitor Article 40 alerts and reviewed the statistics after one full year of operation of the new SIS at the May 2024 meeting. The number of alerts was low and involved only a very few Member States. The low alert level means that a coordinated activity is not required currently, but the DPAs of the Member States can query specific instances at national level to obtain insights on how the alerts are being applied.

The CSC will continue monitoring statistics on the creation of these alerts.

5.5.7 Legal interpretation of provisions of the audit cycle

During 2023, the CSC has started to work on the legal interpretation of Articles 55.2 and 56.2 of SIS Regulation (EU) 2018/1861 and Articles 69.2 and 70.2 of SIS Regulation (EU) 2018/1862 concerning the audit cycle, the extent and comprehensiveness of audit, and the use of international auditing standards. This is an ongoing activity that was inherited by the CSC from the SIS SCG.

This issue is important for all DPAs because the obligation to carry out an audit at regular intervals falls upon the EDPS and national DPAs. Similar audit provisions exist in other legal instruments (for example, EES, ETIAS, interoperability, VIS, etc.), so the outcome of this CSC legal assessment is key to establishing the precise methodology and frequency of the audits that the DPAs should perform for other EU IT systems.

Following preliminary discussion in CSC, a draft proposal for a common approach is being prepared for further consideration in the committee.

5.5.8 Commission Schengen Evaluation

The European Commission, represented by officials from DG JUST and DG HOME, made a presentation to the CSC at their September 2023 meeting. The new SIS was described along with the existing tools that were available to support Member States to implement the system.

The presentation covered the new Schengen Evaluation

23. Article 36 of [Regulation \(EU\) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System \(SIS\) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation \(EC\) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU](#).

24. https://www.edpb.europa.eu/our-work-tools/our-documents/csc-documents/report-article-36-alerts-schengen-information-system_en

25. Article 40 [ibid](#).

Framework (SCHEVAL)²⁶. Issues raised during the presentation included the composition of the SCHEVAL pool of experts, training, exchange of relevant information, thematic evaluations, and the security accreditation of experts. The CSC has continued to cooperate with the Commission through training of data protection experts and the organisation of evaluation exercises for training purposes.

In the July 2024 CSC meeting the European Commission presented the Schengen Scoreboard, the KOEL platform set up to facilitate exchange of communication among the Member States and the Commission and some additional issues including an exchange on the experience from recent SCHEVAL evaluations conducted under the new methodology, the inspection plan for the next few years and the state of play of implementation of EES/ETIAS into SCHEVAL.

5.5.9 eu-LISA information sharing

The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) was established to provide a long-term solution for the operational management of large-scale EU IT systems, which are essential instruments in the implementation of the asylum, border management and migration policies of the EU.

The CSC promotes regular contact, sharing of information and queries with the eu-LISA's Data Protection Officer (DPO), and considers this an extremely useful part of its supervisory activities enabling it to detect emerging issues and better shape its supervisory activities.

The CSC invited the eu-LISA's DPO to present the status of the new SIS after its first three months of operation, and the Committee aims at further enhancing the cooperation and bilateral exchange on the latest statistics trends. The eu-LISA's DPO reported at the CSC May and July 2024 meeting including extensive information on the first year of entry into operation of the new SIS.

5.6 VIS

During this reporting period, the VIS, was brought under the scope of CSC. The transition of coordinated supervision from the VIS Supervision Coordination Group (SCG)²⁷ to the CSC was successful and seamless.

Currently, the VIS is undergoing a revision, including to enable its integration into the interoperability architecture. The revised VIS is planned to be ready to enter into operation in autumn 2026.

Next year CSC will produce a report dedicated to CSC coordinated activities in 2024 with respect to VIS, and VIS statistics for the period 2022-2024 will be included as an

26. https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-area/schengen-evaluation-and-monitoring_en.

27. https://www.edps.europa.eu/data-protection/european-it-systems/schengen-information-system_en



6. LOOKING AHEAD: CHALLENGES FOR 2024-2026

The CSC will continue to work on the pending actions of its defined 2022-2024 work programme and will develop its next work programme for 2024-2026. With the potential onboarding of several additional EU IT systems and an increased focus on interoperability between IT systems, the workload of the committee will considerably increase.

6.1 Preparation to onboard further existing and new EU-information systems

A number of existing and new EU IT systems are expected to fall within the remit of the CSC over the next few years.

The **Customs Information System (CIS)** is a computer system centralising customs information with the aim of preventing, investigating and prosecuting breaches of Community customs or agricultural legislation. The CIS is composed of a central database accessible through terminals in each Member State.

The CIS is currently under the scope of the Customs Information System Supervision Coordination Group (CIS SCG)²⁸ as set up by Regulation (EC) No 766/2008 to ensure a coordinated supervision in the area of personal data protection of the CIS information system. The EDPS currently provides the secretariat and organisation of meeting for the CIS SCG.

Supervision of relevant CIS activities previously under the scope of the Customs Joint Supervisory Authority were

transferred to CSC in the first half of 2024.

The **Entry-Exit System (EES)** was expected to be launched in November 2024, but its entry into operation have been further postponed. It is a new automated IT system that will replace the physical stamping of passports when entering the EU and other Schengen countries. All EU Member States, except Cyprus and Ireland, and all four EFTA countries (Iceland, Liechtenstein, Norway and Switzerland) will take part. The system will record all entries to and exits from participating European countries with collection of personal data including passport information, facial images and fingerprints.

The **European Travel Information and Authorisation System (ETIAS)** is scheduled to follow shortly afterwards and will be a new entry requirement for visa-exempt nationals travelling to 30 European countries (the EES countries plus Cyprus). An ETIAS authorisation will be linked to the traveller's passport and will be valid for up to three years or until the passport expires. The CSC is already preparing to assume its role as a forum for coordinated supervision in regards of ETIAS.

The **Prüm II Regulation** on automated data exchange for police cooperation was adopted in March 2024. It revises the existing Prüm framework and includes provisions on the automated exchange of DNA profiles, dactyloscopic data, facial images, police records and vehicle registration

28. https://www.edps.europa.eu/data-protection/supervision-coordination/customs-information-systems_en.

data. It also contains new technical infrastructure and extends its participants to include Europol. The CSC is preparing to assume its role as a forum for coordinated supervision in regard to Prüm II.

Further systems – namely, the [European Criminal Records Information System on Third-Country Nationals \(ECRIS-TCN\)](#) and the [European Asylum Dactyloscopy Database \(Eurodac\)](#) will also fall within the remit of the committee along with the continuing coordinated supervision of elements of the interoperability framework.

6.2 Enhanced internal organisation

The CSC currently actively contributes to the coordinated supervision of five EU IT systems, bodies, offices and agencies. In addition, in the near future, the CSC will cover the EES, ETIAS and parts of CIS activities.

With the number of EU IT systems, bodies, offices and agencies under its purview more than doubling, the CSC will need to adapt, which will require much more resources from the EU budget authorities, as it provides the CSC Secretariat. In addition, national DPAs will need to allocate substantially more resources, not only to supervise the data controllers under their purview, but also to support the work required to coordinate supervision at EU/CSC-level.

Going forward, the CSC will be organising more meetings. To ensure an efficient and resourceful coordinated supervision into the future, it will be essential that national DPAs and the EDPS support the work of the CSC, including by ensuring the availability of staff to engage actively within the committee, act as rapporteurs, and lead specific activities, in order to maintain the ability of the CSC to effectively fulfil its legal obligations.

CONTACT DETAILS

Postal address
Rue Wiertz 60, B-1047 Brussels

Office address
Rue Montoyer 30, B-1000 Brussels



**Coordinated
Supervision
Committee**



THE SCHENGEN INFORMATION SYSTEM

A GUIDE FOR EXERCISING DATA SUBJECTS' RIGHTS: THE RIGHT OF ACCESS, RECTIFICATION AND ERASURE

This guide was compiled by the SIS II Supervision Coordination Group.

The national contributions, and any translations of this guide into languages other than English, are the responsibility of each national supervisory authority and they do not necessarily reflect the official position of the CSC. The CSC does not guarantee the accuracy of the information included in the national contributions and any questions should be addressed to the respective national supervisory authorities. Neither the CSC nor any person acting on the CSC's behalf may be held responsible for the use which may be made of the information contained therein.

Secretariat postal address: Rue Wiertz 60, B-1047 Brussels

Offices: Rue Montoyer 30, B-1000 Brussels

E-mail : csc-secretariat@edpb.europa.eu

TABLE OF CONTENTS

1.	Introduction to the Schengen Information System (SIS)	5
1.1.	Legal basis	6
1.2.	Categories of information processed (alerts).....	7
1.3.	Categories of personal data processed	8
2.	Rights recognised to individuals whose data is processed in the SIS.....	9
2.1.	Right of access	10
2.2.	Rights to rectification and erasure of data.....	11
2.3.	Remedies: the right to complain to the data protection authority or to initiate a judicial proceeding.....	12
3.	Description of the procedure for the exercise of the rights in each Schengen State	12
3.1.	AUSTRIA.....	13
3.2.	BELGIUM.....	14
3.3.	BULGARIA.....	17
3.4.	CROATIA.....	20
3.5.	CZECH REPUBLIC.....	22
3.6.	DENMARK	24
3.7.	ESTONIA.....	26
3.8.	FINLAND.....	28
3.9.	FRANCE	30
3.10.	GERMANY.....	33
3.11.	GREECE	35
3.12.	HUNGARY.....	38
3.13.	ICELAND	40
3.14.	IRELAND	42
3.15.	ITALY	45
3.16.	LATVIA.....	47
3.17.	LUXEMBOURG.....	50
3.18.	LIECHTENSTEIN.....	53
3.19.	LITHUANIA.....	55

3.20. MALTA	57
3.21. NETHERLANDS	60
3.22. NORWAY	63
3.23. POLAND	66
3.24. PORTUGAL.....	73
3.25. ROMANIA.....	75
3.26. SLOVAK REPUBLIC.....	78
3.27. SLOVENIA.....	81
3.28. SPAIN.....	84
3.29. SWEDEN.....	88
3.30. SWITZERLAND	90
Annex 1.....	92
Model letter for requesting access	92
Annex 2.....	92
Model letter for requesting rectification	93
Annex 3	94
Model letter for requesting erasure.....	94

Any individual is guaranteed the right of access to his/her own data, the right to rectification of inaccurate data and the right to erasure of unlawfully stored data in the Schengen Information System (hereinafter 'SIS')¹.

This Guide describes the modalities for exercising those rights. This is the most updated version, of 21 November 2022, to reflect the changes brought by the current SIS legal framework and the revision of the EU data protection framework, since the SIS Regulations are now referring to the exercise of some rights as laid down in the GDPR² and in the Law Enforcement Directive³.⁴

The Guide is divided into three sections: (1) a description of the SIS, of (2) the rights granted to the individuals whose data are processed in SIS and (3) a description of the procedure for exercising the rights in each of the countries concerned.

As annex to the Guide, it is also made available three model letters to be used by applicants to file the requests of access, rectification and erasure, unless the national competent authority to which the request is addressed requires the use of a specific standard form.

1. INTRODUCTION TO THE SCHENGEN INFORMATION SYSTEM (SIS)

The SIS is a large-scale IT system, set up as a compensatory measure for the abolition of internal border checks, and intends to ensure a high level of security within the area of freedom, security and justice of the European Union, including the maintenance of public security and public policy and the safeguarding of security in the territories of the Member States. The SIS is already implemented in all EU Member States, with the exception of Cyprus⁵, and in four Associated States: Iceland,

¹ These rights are granted under Article 53 of Regulation (EU) 2018/1861 and Article 67 of Regulation (EU) 2018/1862.

² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1

³ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89.

⁴ Cfr. Article 53 of Regulation (EU) 2018/1861 and Article 67 of Regulation (EU) 2018/1862.

⁵ Information dated from October 2022. Croatia is connected to the SIS with some limitations that are expected to be overcome in 2024. Ireland operates SIS for law enforcement purposes only.

Liechtenstein, Norway and Switzerland.

The SIS is an information system that allows national law enforcement, judicial and administrative authorities to perform their legal tasks by sharing relevant data. With regard to the European agencies, they have read-only access; i.e. the possibility to search and consult the SIS but not to update or delete the data or the alerts. EUROPOL has access to all categories of alerts stored in SIS⁶, while EUROJUST⁷ has access to specific alerts in the field of police and judicial cooperation, and the European Border and Coast Guard (EBCG)⁸ has limited access to the SIS for certain teams and for specific purposes.

1.1. Legal basis

In 2018, the SIS legal framework went through a significant revision primarily to enlarge its purposes, to add certain categories of alerts, and to expand the authorities with granted access to SIS data. The new legal framework was adopted on 28 November 2018 and published on 7 December 2018⁹.

It consists of three new Regulations, covering three areas of competence:

- Regulation (EU) 2018/1860¹⁰ (“SIS Regulation on the use of SIS for the return of illegally staying third-country nationals”)¹¹,
- Regulation (EU) 2018/1861¹² (“SIS Regulation in the field of border checks”)¹³,

⁶ Article 35(1) of Regulation (EU) 2018/1861 and Article 48 (1) of Regulation (EU) 2018/1862.

⁷ Article 49 (1) of Regulation (EU) 2018/1862.

⁸ Article 36 (1) of Regulation (EU) 2018/1861 and Article 50 (1) of Regulation (EU) 2018/1862.

⁹ Initially, they were supposed to become fully applicable by 28 December 2021(Article 20 of Regulation 2018/1860, Article 66 (2) Regulation 2018/1861 and Article 79 of Regulation 2018/1862); however due to delays in the implementation of the new functionalities of the system, the new Regulations only became fully applicable since 7 March 2023.

¹⁰ Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals, OJ L 312, 7.12.2018, p. 1.

¹¹ The SIS Regulation for return is applicable to all Member States and associated Schengen States, with the exception of Ireland.

¹² Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006, OJ L 312, 7.12.2018, p. 14.

¹³ The SIS Regulation in the field of border checks applies to all Schengen States.

- Regulation (EU) 2018/1862¹⁴ (“SIS Regulation in the field of police and judicial cooperation”), as amended by Regulation (EU) 2022/1190¹⁵

The SIS will become, in the near future, interoperable with five other EU-large information systems¹⁶, pursuant to the full application of the Interoperability Regulations¹⁷. This fact, among other things, will have an impact on the exercise of data subjects’ rights in this context. By then, this Guide will be updated accordingly.

1.2. Categories of information processed (alerts)

The SIS contains two broad categories of information: alerts on *persons* and alerts on *objects*. With regard to alerts on persons, SIS covers the following categories of data subjects:

- third country nationals subject to refusal of entry or stay in the Schengen area or subject to return procedures,
- persons wanted for arrest for surrender or extradition purposes (in the case of associated countries),
- missing persons (including vulnerable persons who need to be prevented from travelling, e.g., children at high risk of parental abduction, children at risk of becoming victims of trafficking in human beings, and children at risk of being recruited as foreign terrorist fighters),
- persons sought to assist with a criminal judicial procedure,
- persons subject to discreet, inquiry or specific checks,
- unknown wanted persons who are connected to a crime (e.g. persons whose fingerprints are found on a weapon used in a crime),

¹⁴ Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU, OJ L 312, 7.12.2018, p. 56.

¹⁵ Regulation (EU) 2022/1190 of the European Parliament and of the Council of 6 July 2022 amending Regulation (EU) 2018/1862 as regards the entry of information alerts into the Schengen Information System (SIS) on third-country nationals in the interest of the Union, OJ L 185, 12.7.2022, p. 1.

¹⁶ VIS, Eurodac, EES, ETIAS and ECRIS-TCN.

¹⁷ Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA, OJ L 135, 22.5.2019, p. 27; Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816, OJ L 135, 22.5.2019, p. 85.

- Information on third country nationals in the interest of the Union (“information alerts”).

These last two alerts are brand new in the SIS, introduced by the SIS Recast. While other alerts have been considerably modified by the new legal framework, such as the alert on missing persons or the alert on discreet or specific checks.

With regard to the alerts on objects, SIS stores data on objects sought for the purpose of seizure or use as evidence in criminal proceedings, or subject to discreet or specific checks. Such objects include vehicles, boats, firearms, identity documents stolen, misappropriated, lost or invalidated, bank notes, credit cards, blank documents, and as a new category “objects of high value” (e.g., items of information technology, which can be identified and searched with a unique identification number).

1.3. Categories of personal data processed

When the alert concerns a person (with the exception of unknown wanted person), the information must always include: the surname, date of birth, the reason for the alert, the gender, a reference to the decision giving rise to the alert, the basis for the decision for refusal of entry and stay (when applicable), the action to be taken, last date of the period for voluntary departure if applicable, whether return is accompanied by an entry ban. If available, the alert may also contain information such as, any specific, objective, physical characteristics not subject to change; the place of birth; photographs; fingerprints; nationality(ies); whether the person concerned is armed, violent or has escaped; the authority issuing the alert; links to other alerts issued in SIS in accordance with Article 48 of Regulation (EU) 2018/1861 or Article 63 of Regulation (EU) 2018/1862.

When the alert concerns unknown wanted persons, only dactyloscopic data may be processed, either complete or incomplete sets of fingerprints or palm prints, which due to their unique character and the reference points contained therein should enable accurate and conclusive comparisons on a person's identity¹⁸.

¹⁸ According to the definition provided by Article 3 (13) of Regulation (EU) 2018/1862.

2. RIGHTS RECOGNISED TO INDIVIDUALS WHOSE DATA IS PROCESSED IN THE SIS

Data subjects shall be able to exercise the rights in relation to their personal data processed in the SIS, as laid down in Articles 15, 16 and 17 of the GDPR and in Articles 14 and 16 (1) and (2) of the LED, and in accordance with the SIS Regulations¹⁹. In addition, data subjects are entitled to seek remedies to enforce such rights²⁰.

Therefore, data subjects have the following rights:

- right of access to data relating to them processed in the SIS;
- right to rectification of inaccurate data;
- right to erasure when data have been unlawfully stored;
- right to bring an action before the courts or competent supervisory authorities to access, rectify, erase, obtain information or obtain compensation in connection to an alert concerning them.

Anyone exercising any of these rights can apply to the competent authorities in a Schengen State of his or her choice. This option is possible because all national databases (N.SIS) are identical to the central system database (CS.SIS)²¹. Consequently, these rights can be exercised in any Schengen country regardless of the State that issued the alert.

However, the Member State receiving the request from the data subject has to consult previously the Member State issuing the alert before providing any information to the data subject about the data processed in the SIS.

To assist data subjects in exercising their rights, this Guide publishes in its Part 3 the list of national authorities competent to handle data subjects' requests, how these are to be addressed, including any national requirements, and what means are made available for that purpose.

Regardless of specific national procedures to handle the application for access, rectification or erasure of data processed in the SIS, the reply to the data subject is due within a strict common

¹⁹See 53 of Regulation (EU) 2018/1861 and 67 of Regulation (EU) 2018/1862.

²⁰See Article 54 of Regulation (EU) 2018/1861 and Article 68 of Regulation (EU) 2018/1862.

²¹ See Article 4(1)(b) of Regulation (EU) 2018/1861 and of Regulation (EU) 2018/1862.

deadline. The data subject shall be informed as soon as possible, and, in any event, within one month of receipt of the request, about the follow-up given to the exercise of the right. This period may be extended by two further months where necessary and in such case, the data subject shall be informed of any such extension within one month of receipt of the request, together with the reasons for the delay²².

2.1. Right of access

The right of access is the possibility for anyone who so requests to have knowledge of whether or not information relating to him or her are processed by a public or private organisation, and to receive information on these data. This is a fundamental right, enshrined in Article 8 (2) of the EU Charter of Fundamental Rights, and its exercise is instrumental to put into effect other data protection rights and to protect in general the freedoms and rights of individuals.

The right of access in what concerns the data processed in the SIS is provided for in Article 53(1) of Regulation (EU) 2018/1861 and in Article 67(1) of Regulation (EU) 2018/1862²³, which refer to the right of access laid down in Article 15 of the GDPR and Article 14 of the LED.

This means that data subjects have the right to obtain confirmation as to whether or not personal data concerning them are being processed in the SIS and, where that is the case, access to the personal data and the following information:

- The purpose of the processing;
- The categories of personal data concerned;
- The recipients or categories of recipients to whom the personal data have been disclosed, in particular in third countries or international organisations;
- The envisaged period for which the personal data will be stored;
- The existence of the right to request rectification of inaccurate data or erasure of unlawfully stored data;
- The right to lodge a complaint

²² See Article 53(4) of Regulation (EU) 2018/1861 and 67(4) of Regulation (EU) 2018/1862, which refers to the deadlines provided in Article 12(3) of the GDPR.

²³ Both Articles state : 'Data subjects shall be able to exercise the rights laid down in Articles 15 (...) of Regulation (EU) 2016/679 and in Article 14 (...) of Directive (EU) 2016/680 [...]'

- Communication of the source of the information when data is collected from a third party.

However, the right of access is exercised in accordance with the law of the Member State where the request is submitted, and there could be restrictions to access the data, i.e. a decision not to provide information, wholly or in part, to the data subject. This is possible to the extent that such limitation constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the data subject concerned, in order to:

- avoid obstructing official or legal inquiries, investigations or procedures;
- avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- protect public security;
- protect national security; or
- protect the rights and freedoms of others²⁴.

Where that is the case, the applicant shall be informed in writing, without undue delay, of any refusal or restriction, unless the provision of such justification undermines one of the above-mentioned objectives. The authority receiving the request for access shall inform the applicant that he or she can lodge a complaint with the data protection authority or seek judicial remedy.

If there is a complete or partial refusal of access, data subjects can exercise their rights vis-à-vis the SIS through the national data protection supervisory authority. This Guide also publishes the name and contact details of the data protection supervisory authorities in each Schengen State.

2.2. Rights to rectification and erasure of data

Besides the right of access, there is also the right to obtain the rectification of personal data factually inaccurate or incomplete or the right to ask for erasure of personal data unlawfully stored (Article 53(1) of Regulation (EU) 2018/1861 and Article 67(1) of Regulation (EU) 2018/1862).

Under the Schengen legal framework, only the Member State responsible for issuing an alert in the SIS may alter or delete it (See Article 44(3) of Regulation (EU) 2018/1861 and 59(3) of Regulation (EU) 2018/1862).

²⁴ See Articles 53(3) of Regulation (EU) 2018/1861 and 67(3) of Regulation (EU) 2018/1862.

If the request is submitted in a Member State that did not issue the alert, the competent authorities of the Members States concerned cooperate to handle the case, by exchanging information and making the necessary verifications.

The applicant should provide the grounds for the request to rectify or erase the data and gather any relevant information supporting it.

2.3. Remedies: the right to complain to the data protection authority or to initiate a judicial proceeding

Articles 54 of Regulation (EU) 2018/1861 and 68 of Regulation (EU) 2018/1862 presents the remedies accessible to individuals when their request has not been satisfied. Any person may bring an action before the courts or the authority competent under the law of any Member State to access, rectify, erase, obtain information or to obtain compensation in connection with an alert relating to him or her.

In case they have to deal with a complaint with a cross-border element, supervisory authorities should cooperate with each other to guarantee the rights of the data subjects.

3. DESCRIPTION OF THE PROCEDURE FOR THE EXERCISE OF THE RIGHTS IN EACH SCHENGEN STATE

The procedures specific to each country applying the Schengen acquis, which are to be followed by individuals wishing to exercise their right of access, rectification or erasure, are described in the national fact sheets in the remainder of this chapter.

3.1. AUSTRIA

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Bundesministerium für Inneres (BMI)
Bundeskriminalamt, SIRENE Österreich
Josef Holaubek Platz 1
1090 Vienna
AUSTRIA
E-Mail: bundeskriminalamt@bmi.gv.at

2. How to make an individual request and what to include in it?

In Austria, the right to access is direct. A request for access must be made to the Bundesministerium für Inneres (Ministry of the Interior), which is the authority responsible for the national system of the Schengen Information System.

The request has to be made in writing and must contain the signature of the applicant. The request must be accompanied by a copy of a valid and official identity document, which has to contain the name, date of birth, photograph and signature of the applicant (e.g. passport, identity card or driving licence). The Datenschutzbehörde (Austrian Data Protection Authority) provides a template (in German and English) on its website (www.dsb.gv.at). The request of access is free.

If the Ministry of the Interior does not take action on the request of the applicant within four weeks or the applicant is of the opinion that the provided information of the Ministry of the Interior is incomplete or wrong, the applicant can lodge a complaint with the Austrian Data Protection Authority.

In accordance with the Austrian constitution, the official language in Austria is German. However, the request can also be made in English.

3. Contact details of the national data protection authority

Datenschutzbehörde
Barichgasse 40-42
1030 Vienna
Austria
E-mail: dsb@dsb.gv.at
Website: www.dsb.gv.at

4. Expected outcome of requests for access. Content of the information supplied

In accordance with § 44 of the Data Protection Act, every data subject shall have the right to obtain confirmation from the controller as to whether personal data concerning him or her are being processed; if this is the case, he or she shall have the right to obtain access to personal data.

In the event of a refusal to provide the information, the controller shall pursuant to § 43(4) of the Data Protection Act immediately inform the data subject in writing of the refusal or restriction of the information and the reasons for it. This shall not apply if the provision of such information would be contrary to one of the purposes mentioned in § 43(4) of the Data Protection Act, i.e. to ensure that the prevention, detection, investigation or prosecution of criminal offences or the execution of sentences are not impaired, in particular by obstructing official or judicial enquiries, investigations or proceedings, for the protection of public and national security, for the protection of the constitutional institutions of the Republic of Austria, for the protection of military self-security, or for the protection of the rights and freedoms of others. The controller shall inform the data subject of the possibility to lodge a complaint with the data protection authority.

5. References of the main national laws that apply

[Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten \(Datenschutzgesetz – DSG\)](#)

3.2. BELGIUM

The exercise of the rights of access, rectification and deletion concerning SIS differs according to whether the alert is processed for the purpose of refusing admission or a ban on residence in the Schengen area or for the purposes of police and judicial cooperation in criminal matters.

If the request concerns an alert processed for the purposes of refusing admission or a stay in the Schengen area or return resulting from an administrative decision taken by the Belgian Immigration Office, it must be addressed to the Immigration Office, Federal Public Service Interior, CSIS Office.

In the absence of a response from the CSIS Office within the period of one month from the receipt of your request or if this answer is not satisfactory, you can lodge a complaint with the Data Protection Authority (<https://www.dataprotectionauthority.be/citizen>).

If your request concerns another alert introduced by the Belgian authorities (for the purposes of police and judicial cooperation in criminal matters), it must be sent to the Supervisory Body for Police Information.

Concerning the purposes of police and judicial cooperation in criminal matters, Belgium has a system of indirect access. It means that the request must be sent to the Supervisory Body which verifies the data. According to the Belgian data protection Act (30 July 2018), the Supervisory Body only communicates to the person concerned that the necessary checks have been carried out.

1. Contact details of the body to which requests for access, correction or deletion should be addressed

For the purposes of police and judicial cooperation in criminal matters:

Supervisory Body for Police Information
Rue de Louvain 48, 1000 Brussels, Belgium
+32 (0)2 549 94 20
Info@organedecontrole.be

For the other purposes :

Immigration Office, Federal Public Service Interior
CSIS Office
Boulevard Pacheco 44, 1000 Brussels, Belgium
e-mail: csis@ibz.fgov.be

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

- Data subject.
- Lawyer with power of attorney.

2.2. To whom the request should be submitted

- Concerning the purposes of police and judicial cooperation in criminal matters, the request should be sent to the Supervisory Body which verifies the data.
- Concerning the other purposes, it must be addressed to the Immigration Office, Federal Public Service Interior, CSIS Office.

2.3. How the request should be submitted

- In paper and/or electronic format, digitally signed;

- It must be written, dated and signed by the data subject or his lawyer;
- Concerning the purposes of police and judicial cooperation in criminal matters, the request can be submitted via an online form: <https://www.controleorgaan.be/en/citizens/access-to-the-schengen-information-system-sis-ii> ;
- Concerning the other purposes, it must be addressed via e-mail (csis@ibz.fgov.be)
- Any additional information can be provided within one month of the request.

2.4. Minimum information to be supplied

- Personal data of the applicant (name, surname, date of birth, nationality, gender, citizenship);

2.5. Documents to be supplied

- The data subject must also provide proof of identity by attaching a copy of an identity document (double-sided);
- A lawyer must provide evidence of his capacity and also attach the mandate given by his client.

2.6. Language regime

- The request can be submitted in one of the Belgian national languages or in English ;
- The reply to the applicant will be in one of the Belgian national languages or in English.

2.7. Link to website where information on how to apply for information/correction/deletion

Concerning the Supervisory Body for Police Information :

<https://www.controleorgaan.be/en/citizens/access-to-the-schengen-information-system-sis-ii>

Concerning the Immigration Office, Federal Public Service Interior : <https://dofi.ibz.be/>

3. Contact details of the national data protection authority

Concerning the purposes of police and judicial cooperation in criminal matters :

Supervisory Body for Police Information

Control and supervisory authority for the processing of data by the police, in particular in the context of the SIS

Rue de Louvain 48, 1000 Brussels, Belgium

+32 (0)2 549 94 20

Info@organedecontrole.be

www.organedecontrole.be

Concerning the other purposes :

Data Protection Authority

Rue de la Presse, 35

1000 Bruxelles

+32 (0)2 274 48 00

+32 (0)2 274 48 35

contact@apd-gba.be

www.dataprotectionauthority.be

4. Expected outcome of requests for access. Content of the information supplied

4.1. Content of the notifications

The exercise of the rights of access, rectification and deletion concerning SIS differs according to

whether the alert is processed for the purpose of refusing admission or a ban on residence in the Schengen area or for the purposes of police and judicial cooperation in criminal matters.

If the request concerns an alert processed for the purposes of refusing admission or a stay in the Schengen area or return resulting from an administrative decision taken by the Belgian Immigration Office, it must be addressed to the Immigration Office, Federal Public Service Interior, CSIS Office.

If your request concerns another alert introduced by the Belgian authorities (for the purposes of police and judicial cooperation in criminal matters), it must be sent to the Supervisory Body for Police Information.

Concerning the purposes of police and judicial cooperation in criminal matters, Belgium has a system of indirect access. This signifies that the request must be sent to the Supervisory Body which will verify the data. According to the Belgian data protection Act (30 July 2018), the Supervisory Body only communicates to the person concerned that "*the necessary checks have been carried out*". The Supervisory Body can therefore never provide you with any concrete information concerning the processed data.

4.2. Procedure to submit a complaint

Concerning the purposes of police and judicial cooperation in criminal matters, the Belgian data protection Act provides for a procedure in Article 209.

This action must be brought against the controller.

Concerning the other purposes, in the absence of a response from the CSIS Office within the period of one month from the receipt of your request or if this answer is not satisfactory, a complaint can be lodged with the Data Protection Authority (<https://www.dataprotectionauthority.be/citizen>).

5. References of the main national laws that apply

5.1 Act on the protection of natural persons with regard to the processing of personal data, 30 July 2018

5.2 Specific elements

The exercise of the rights of access, rectification and deletion concerning SIS II differs according to whether the alert is processed for the purpose of refusing admission or a ban on residence in the Schengen area or for the purposes of police and judicial cooperation in criminal matters.

Concerning the purposes of police and judicial cooperation in criminal matters, Belgium has a system of indirect access. It means that the request should be sent to the Supervisory Body which verifies the data. According to the Belgian data protection Act, the Supervisory Body only communicates to the person concerned that the necessary checks have been carried out.

Concerning the other purposes, this a direct procedure with the Immigration Office, Federal Public Service Interior, CSIS Office.

3.3. BULGARIA

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Ministry of Interior of the Republic of Bulgaria

SIRENE Bureau at the Ministry of Interior (International Operational Cooperation Directorate)

Address: 1146 Knyaginya Maria Luiza Blvd, Sofia 1233, Bulgaria

Tel.: +359 2 9825 000

Fax: +359 2 9153 525

Email: priemna@mvr.bg

Web site: <https://www.mvr.bg/>

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

Every individual has the right of access to his/her personal data, processed in Ministry of Interior's (Mol) information funds or SIS.

The individual should submit access request directly to the national SIRENE Bureau, established as a unit in the International Operative Cooperation Directorate of the Mol.

Such request could be submitted to the Commission for Personal Data Protection (CPDP) as well, which will forward it to the Mol.

2.2. How the request should be submitted

The request can be submitted in person, on paper (via post) and/or in electronic format signed with qualified electronic signature by the data subject, by lawyer with power of attorney or legal guardian, if necessary. The data subjects can be represented by appointed lawyer or legal guardian.

On CPDP's official site are provided model letters for requesting information from SIS II, as follows:
<https://www.cpdp.bg/en/index.php?p=element&aid=1310> – In English

The Minister of Interior is obliged to take a decision within 14 days from the receipt of the access request. A copy of the individual's processed personal data can be provided on paper upon request. The submission of request for access to SIS data is free of charge.

2.3. Minimum information to be supplied

The minimum supplied applicant personal data is: name, surname, date of birth, nationality, gender, citizenship and information about passport validity.

Model forms for exercising the rights of access, correction or deletion of data can be found on the CPDP's official site:

<https://www.cpdp.bg/en/index.php?p=element&aid=1310> – in English

In the model letters as reasons for the correction/deletion of personal data are set inaccuracy or unlawful storage.

2.4. Documents to be supplied

The documents that need to be supplied for the request are:

- proof of applicant's identity- readable copy of ID or passport
- proof of granted power of attorney- when necessary
- notarial verified letter of attorney (in case of authorisation of representation by third party)

2.5 Language regime

The languages that can be used when submitting the request are Bulgarian and English. The language used to reply to the applicant if he/she isn't Bulgarian citizen is English.

2.6. Link to website where information on how to apply for information/correction/deletion

The link to apply for information/correction/deletion of personal data in SIS II is:
<https://www.cpdp.bg/en/index.php?p=element&aid=1310> – in English

3. Contact details of the national data protection authority

Commission for Personal Data Protection
Sofia 1592, 2 "Prof. Tsvetan Lazarov" blvd.
Tel.: + 3592/91-53-519
Fax: +3592/91-53-525
E-mail: kzld@cpdp.bg
Web site: www.cpdp.bg.

4. Expected outcome of requests for access. Content of the information supplied

4.1. Content of the notifications

In accordance with Art. 15 (1) and (2) of the in Ordinance No. 81213-465 of 26 August 2014 on the organization and functioning of the National Schengen Information System of the Republic of Bulgaria (Prom. SG 74/5 September 2014, last amend. and suppl. SG 23/22 March 2022), the data subject has right to access, correct or request deletion of his/her inaccurate or unlawfully processed personal data in N.SIS.

The data subjects' rights are exercised under the conditions and following the procedures set in the Regulation (EU) 2018/1860, Regulation (EU) 2018/1861, Regulation (EU) 2018/1862, Ministry of Interior Act and the Personal Data Protection Act.

4.2. Procedure to submit a complaint

Complaints about violations of the individual's rights for access, correction or deletion of his/her personal data in SIS II can be submitted following the requirements described on the CPDP's official site:
<https://www.cpdp.bg/en/index.php?p=pages&aid=56> - in English

5. References of the main national laws that apply

- Ministry of Interior Act (MIA) (Prom. SG 52/27 June 2014, last amend. and suppl. SG 62/5 August 2022) and the related secondary legislation - e.g. the specific rules for the organization and operation of the national system (N.SIS) are set out in Ordinance No. 81213-465 of 26 August 2014 on the organization and functioning of the National Schengen Information System of the Republic of Bulgaria (Prom. SG 74/5 September 2014, last amend. and suppl. SG 23/22 March 2022). In accordance with Article 14 of the Ordinance, data processing at N.SIS is carried out in compliance with the Regulation (EU) 2018/1860, Regulation (EU) 2018/1861, Regulation (EU) 2018/1862, Ministry of Interior Act and the Personal Data Protection Act and the subsidiary legislation, related to their application.

Certain aspects of personal data protection, related to SIS II, are also regulated by other legal acts, such as:

- the Administrative Procedure Code (Prom. SG 30/11 April 2006, last amend. and suppl. SG 15/19 February 2021)- judicial control;
- the Penal Code (Prom. SG 26/2 April 1968, last amend. and suppl. SG 53/8 July 2022);
- the Penal Procedure Code (Prom. SG 83/18 October 2005, last suppl. SG 62/5 August 2022);
- the Foreigners in the Republic of Bulgaria Act (Prom. SG 153/23 December 1998, last amend. SG 22/18 March 2022);
- the Extradition and European Arrest Warrant (EAW) Act (Prom. SG 46/3 January 2005, last amend. and suppl. SG 45/7 June 2019);
- the Bulgarian Personal Documents Act (Prom. SG 93/11 August 1998, last amend. SG 32/26 April 2022);
- the Customs Act (Prom. SG 15/6 February 1998, last suppl. SG 62/5 August 2022);
- the State Agency for National Security Act (Prom. SG 109/20 December 2007, suppl. SG 51/5 June 2020);
- the Act on entering, residing and leaving the Republic of Bulgaria by European Union citizens and their family members (Prom. SG 80/3 October 2006, amend. and suppl. SG 21/12 March 2021);
- Asylum and Refugees Act (Prom. SG 54/31 May 2002, last amend. SG 32/26 April 2022);
- the Administrative Violations and Penalties Act (Prom. SG. 92/28 November 1969, last suppl. SG 51/1 July 2022- judicial control.

The requests for access/correction/deletion of personal data in N.SIS can be send in Bulgarian and English.

The alerts storage deadlines can be prolonged in case it is necessary for the achievement of their purposes. The prolongation necessity is revised by the authority, which has entered the alert one month after the set deadlines have expired (for alerts on persons) and after the expiration of the half storage term and two months before the deadline expiration (for alerts on objects- discreet checks and for or seizure or use as evidence in criminal proceedings).

With regard to third country citizens alerts with imposed restrictions for entering and stay (alerts for persons for arrest, for surrender or extradition purposes) the necessity for prolongation is revised within three/five years from their entering depending on the imposed restrictions deadlines.

The SIS alerts for persons and objects are automatically deleted after the set storage deadline under the conditions set in Art.55 of Regulation (EU) 2018/1862, if the further retention is not necessary.

The alerts for third country citizens, who are with revoked right to stay in Bulgaria or are due to be returned to their country or expulsed are deleted under the conditions set in Art.6 (2), Art. 8, it."b", Art. 9 (2), Art. 11, it. "f" and Art. 14 of Regulation (EU) 2018/1860.

The alerts for third country citizens, who are prohibited to enter and reside on the territory of Member States of the European Union or are subject to issued orders for imposition of compulsory administrative measures are deleted under the conditions set in Art. 40 of Regulation (EU) 2018/1861.

In cases of identity theft and the additional processing of the victim personal data, these data are deleted simultaneously with the relevant alert or earlier upon victim's request.

3.4. CROATIA

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Contact details of Ministry of the Interior, the body to which request for access, correction or deletion should be addressed is:

Ministarstvo unutarnjih poslova
Ulica grada Vukovara 33
HR - 10 000 Zagreb

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

Only natural person – data subject can submit a request. It is not envisaged that request can be submitted by layer with power of attorney or legal guardian.

2.2. How the request should be submitted

Request must be submitted in written form to the data controller using templates available on its web site:

- Access https://mup.gov.hr/UserDocsImages//dokumenti/zastita_podataka/29-03//Zahtjev%20za%20pristup%20osobnim%20podacima%20koji%20su%20obra%C4%91eni%20u%20SISII.pdf
- Correction: https://mup.gov.hr/UserDocsImages//dokumenti/zastita_podataka/29-03//Zahtjev%20za%20ispravak%20osobnih%20odataka%20koji%20su%20obra%C4%91eni%20u%20SISI.pdf
- Deletion: https://mup.gov.hr/UserDocsImages//dokumenti/zastita_podataka/29-03//Zahtjev%20za%20brisanje%20osobnih%20odataka%20koji%20su%20obra%C4%91eni%20u%20SISII.pdf

Data subjects must send an application personally signed to the data controller using regular post service. It is not envisaged that request can be submitted by e-mail.

If data subject submit request for access, correction or deletion to national Data Protection Authority, same Authority informs data subject that he/she needs to submit request to Ministry of Interior using forms available on their web site.

2.3. Minimum information to be supplied

Personal data of applicant that should be included are: name, surname, Personal Identification Number (if any), place of residence, place of birth, date of birth, nationality.

2.4. Documents to be supplied

- Documents that should be supplied as proof of identity: copy of ID or passport. Also, applicants do not need to justify their request for access/correction/deletion.

2.5 Language regime

Form is written in Croatian and English languages so it is expected that applicant can submit request on both languages. Consequently, language used for submitting request will be used for providing reply to applicant.

Structured information on how to apply for information/correction/deletion is available on both Croatian

and English versions of web site of Ministry of Interior:

- <https://mup.gov.hr/zastita-osobnih-podataka/222>
- <https://mup.gov.hr/personal-data-protection/124>

2.6. Link to website where information on how to apply for information/correction/deletion

Document specifically related with topic is further available on link:
<https://mup.gov.hr/UserDocsImages//dokumenti//Data-protection-and-the-Schengen-Information-System.pdf>

3. Contact details of the national data protection authority

Agencija za zaštitu osobnih podataka

Selska cesta 136,

10000 Zagreb

Croatia

Tel: +385 1 4609-000

Fax: +385 1 4609-099

www.azop.hr

The Croatian Personal Data Protection Agency (hereinafter: the Agency) is the only independent public supervisory authority in the Republic of Croatia within the meaning of the provision of Article 51 of the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016.

5. References of the main national laws that apply

Croatia does not have separate national Law and it provisions that applies specifically to SIS.

The Act on the Implementation of the General Data Protection Regulation (Official Gazette, No. 44/2018) (Zakon o provedbi Opće uredbe o zaštiti podataka (Narodne Novine 44/2018 https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html) stipulates in Art. 34. that anyone who considers that any of his or her rights guaranteed by the GDPR and the Act on the Implementation of the GDPR have been violated, may submit to the Agency a request for determination of a violation of a right. The Agency shall decide on the violation of rights by a ruling. The ruling of the Agency shall be an administrative act. No appeal shall be allowed against the ruling of the Agency, but an administrative dispute may be instituted by lodging a complaint before a competent administrative court.

If data subject considers that his rights on request for information/correction/deletion in SIS have been violated by Ministry of Interior, he/she can submit claim to the Agency.

3.5. CZECH REPUBLIC

1. Contact details of the body to which requests for access, correction or deletion should be addressed

The Police Presidium of the Czech Republic
P. O. BOX 62/K-SOU, 170 89 Praha 7, Czech Republic
+420 974 835 775
epodatelna.policie@pcr.cz

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

Requests can be submitted by a subject whose data are concerned, or by another person, who has been authorized by the subject.

2.2. How the request should be submitted

Request should be submitted in a written form (paper or digital). It is also possible to submit a request during office hours at any police station.

Link to online forms: <https://www.policie.cz/docDetail.aspx?docid=22450996&doctype=ART>

2.3. Minimum information to be supplied

Identification data, i.e., name and surname, date of birth, address of residence or other postal address usable for delivery shall be supplied. In case of request for data correction or deletion, the justification for the request should be provided, e.g., corrections required, description of circumstances, reasoning for deletion.

2.4. Documents to be supplied

A readable copy of any identification document should be enclosed.

If the data subject authorises another person to submit the request, a special power of attorney with a certified signature must be submitted. In cases where the data subject authorises a lawyer to submit the request, it is sufficient to provide a general power of attorney without a certified signature..

2.5 Language regime

The subject can submit his/ her request either in Czech or in English. The reply is sent to the data subjects in the Czech language.

2.6. Link to website where information on how to apply for information/correction/deletion

Information on how to apply for information, correction or deletion is available on the websites of the Police of the Czech Republic (<https://www.policie.cz/docDetail.aspx?docid=22450996&doctype=ART>) and the Czech national data protection authority (https://www.uouu.cz/en/vismo/zobraz_dok.asp?id_org=200156&id_ktg=1366&p1=1366).

3. Contact details of the national data protection authority

The Office for Personal Data Protection (Úřad pro ochranu osobních údajů)

The Office for Personal Data Protection is competent to review personal data processing within the national part of the SIS at the request of data subjects in cases where there is suspicion of an unlawful

procedure or where the controller (the Police of the Czech Republic) has not provided a satisfactory response.

Pplk. Sochora 27
170 00 Praha 7
Czech Republic
+420 234 665 111
posta@uoou.cz
www.uouu.cz

4. Expected outcome of requests for access. Content of the information supplied

4.1. Content of the notifications

The Police shall answer whether any personal data concerning the data subject is contained in the SIS, what data it is, why it has been entered (for what purpose) and by which authority.

According to the § 28 (3) of the Act No 110/2019 Coll., on Personal Data Processing, the Police must not grant the request if this would jeopardize the accomplishment of police tasks in connection with criminal proceedings or national security or endanger legitimate interests of a third person.

4.2. Procedure to submit a complaint

If the subject does not receive a response from the controller in time or if the response is not satisfactory to the subject, he or she may contact the Office for Personal Data Protection with a complaint. Such a complaint can be submitted in person or in writing (in paper or digital form), in both Czech and English. The data subject shall prove his/her identity and provide all information supporting his/her complaint, e.g., previous communication with the data controller, including documents provided or received. Where the data subject authorises another person to submit a complaint, a special power of attorney with a certified signature must be submitted, except in the case of representation by a lawyer, where a general power of attorney will suffice.

5. References of the main national laws that apply

- Act No. 110/2019 Coll., on Personal Data Processing
- Act No 273/2008 Coll., on the Police of the Czech Republic

3.6. DENMARK

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Requests for access should be addressed to the Danish National Police:

Danish National Police
Polititorvet 14
DK-1780 København V
E-mail: pol-jur-efterforskning@politi.dk
Tel.: +45 33 14 88 88

Request for correction or deletion should be addressed to the Danish Return Agency:

The Danish Return Agency
Birkerød Kongevej 2
DK-3460 Birkerød
Tel.: + 45 30 65 78 00

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

Data subjects, persons or legal entities with a power of attorney, or a legal guardian can submit a request.

2.2. How the request should be submitted

There are no particular formal requirements for submitting a request. However, if at all possible, requests should be submitted electronically through the following secure contact form:

- [Request-for-access](#)
- [Request for correction or deletion](#)

2.3. Minimum information to be supplied

- Personal data of the applicant (name, surname, date of birth, nationality, contact information);
- use of model forms to exercise the rights vis-à-vis the SIS
- in case of request for data correction or deletion, the justification for the request (e.g. corrections required, description of circumstances, reasoning for deletion)

2.4. Documents to be supplied

- proof of applicant's identity (e.g. readable copy of ID, passport, residence permit, birth certificate, drivers' licence);
- proof of granted power of attorney

2.5 Language regime

Danish is the official language used for communication with the Danish authorities. However, it is also possible to communicate with the Danish authorities in English.

2.6. Link to website where information on how to apply for information/correction/deletion

For information on how to submit a request, see the websites listed below:

- [Schengen Information System \(SIS II\) \(datatilsynet.dk\)](https://www.datatilsynet.dk)
- [International police cooperation | Danish police \(politi.dk\)](https://www.politi.dk)
- <https://www.hjemst.dk/kontakt/>

3. Contact details of the national data protection authority

Datatilsynet
Carl Jacobsens Vej 35
DK-2500 Valby
Tel.: +45 3319 3200
Fax: +45 3319 3218
E-mail: dt@datatilsynet.dk
www.datatilsynet.dk

4. Expected outcome of requests for access. Content of the information supplied

4.1. Content of the notifications

The controller (in this case the Danish National Police) will – if not prevented by other interests cf. article 15 of Law Enforcement Directive - inform the data subject whether or not data relating to him/her is being processed in SIS.

4.2. Procedure to submit a complaint

The applicant can submit a complain to the Danish Data Protection Agency if the applicant is dissatisfied with a decision made by the Danish National Police concerning request to access or a decision made by the Danish Return Agency concerning request to correction or deletion of data.

If the applicant wishes to file a complaint, the applicant must provide the following information:

- a description of the nature of the complaint
- a copy of the decision or response that the applicant has received from the Danish National Police or the Danish Return Agency
- any other material that the applicant think is relevant to the complaint

The applicant can also use the Danish Data Protections complaint form:

- [Complaint form.pdf \(datatilsynet.dk\)](https://www.datatilsynet.dk)

5. References of the main national laws that apply

- Act No. 502 of 23 May 2018 on the Data Protection Act
- Act No. 410 of 27 April 2017 on the Law Enforcement Act

3.7. ESTONIA

1. Contact details of the body to which requests for access, correction or deletion should be addressed

For direct access:

Politsei- ja Piirivalveamet (Police and Border Guard Board)
Pärnu mnt 139, Tallinn, 15060
ppa@politsei.ee

For indirect access:

Andmekaitse Inspektsioon (Data Protection Inspectorate)
Tatari 39, Tallinn, 10134
info@aki.ee

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

Request can be submitted by data subjects, legal guardians or persons with the power of attorney.

2.2. How the request should be submitted

There is no formal form for the request, nevertheless there are sample forms [here](#) and [here](#) (in Estonian) that could be filled in. The request should be in written form, preferably electronically.

2.3. Minimum information to be supplied

- A signed application must be submitted to request, correct or delete data entered in the Schengen Information System. The application must state the requester's name, date of birth, nationality and a copy of the identification document attached.
- Justification of the request when requesting deletion or correction of the data.

2.4. Documents to be supplied

- Copy of the identification document

2.5 Language regime

- The requests must be submitted in Estonian.
- In case the request is submitted in English, the controller responds to the applicant in Estonian.

2.6. Link to website where information on how to apply for information/correction/deletion

Please see more information on the websites of [DPI](#) and [PBGB](#).

3. Contact details of the national data protection authority

Andmekaitse Inspektsioon (Data Protection Inspectorate)
Tatari 39, Tallinn, 10134
info@aki.ee

4. Expected outcome of requests for access. Content of the information supplied

4.1. Content of the notifications

The controller (PBGB) will notify the requester in case there is no data in the national register, unless prevented by law.

4.2. Procedure to submit a complaint

In case the requester is not satisfied with the reply or does not get any reply from the controller within 30 days after sending the request, the requester has the right to lodge a complaint with the Data Protection Inspectorate or an administrative court. Filing a complaint with the Data Protection Inspectorate is free of charge. The complain form is found on [DPI's website](#).

5. References of the main national laws that apply

- [Isikuandmete kaitse seadus](#) (Personal Data Protection Act)
- [Haldusmenetluse seadus](#) (Administrative Procedure Act)

3.8. FINLAND

1. Contact details of the body to which requests for access, correction or deletion should be addressed

The National Police Board
PO Box 1000 (Vuorimiehetie 3), 02151 ESPOO
+358 295 480181
kirjaamo.poliisihallitus@poliisi.fi

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

Data subject can submit a request, and he / she can bring along an assistant.

2.2. How the request should be submitted

Applications must be made to the police in person and applicants must at the same time produce proof of identity.

Exercise of the right of inspection is subject to payment only if less than one year has elapsed since the person concerned last exercised that right.

The form can be accessed here: [Use of right of access \(poliisi.fi\)](#)

Applicants will be told if their request cannot be granted immediately when they make the request. The controller will let the applicants know when and how they will be given access to their data.

2.3. Minimum information to be supplied

Personal identity code (or date and place of birth), family name (also previous family name), given names (also previous given names), contact information (address, phone number, email)

The police has templates for exercising the right of access. You do not need to use the templates, however, but can also prepare your own document. Whether you use the police's templates or draw up your own document, your request must specify which of your data you wish to access.

In case of request for data correction or deletion, the justification for the request: request need to contain enough detail about whose personal data are at issue, which data of the police you want rectified or erased, why you feel that the information in question is incomplete, inaccurate or incorrect in view of the purpose of the processing, and how you want the information in question changed.

2.4. Documents to be supplied

- Proof of applicant's identity (e.g. driving licence, identity card, passport (only accepted means of identification outside Finland)).

2.5 Language regime

The request can be made either in Finnish, Swedish or English.

The applicant is replied using the same language used to make the request.

2.6. Link to website where information on how to apply for information/correction/deletion

[Data protection and processing of personal data - Police \(poliisi.fi\)](#)

3. Contact details of the national data protection authority

The office of the Data protection Ombudsman
Street address: Lintulahdenkuja 4, 00530 Helsinki
Postal address: PL 800, 00531 Helsinki, Finland
+358 29 566 6700
tietosuoja@om.fi
www.tietosuoja.fi

4. Expected outcome of requests for access. Content of the information supplied

4.2. Procedure to submit a complaint

You can ask the Data Protection Ombudsman to check the lawfulness of your personal data and the way in which they are being processed if your right of access has been postponed, restricted or denied or if the controller refuses to comply with your request to correct inaccuracies, supplement, erase or restrict the processing of your data

5. References of the main national laws that apply

- Act on the Processing of Personal Data by the Police
- Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security
- Data Protection Act

Restrictions on the right of access

The right to access your data can be denied in certain circumstances. The right of access can be restricted when such a restriction, considering your rights, is necessary and proportionate to safeguard

- the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties,
- another official investigation, audit or other such procedure,
- public security,
- national security, or
- the protection of the rights of others.

3.9. FRANCE

1. Contact details of the body to which requests for access, correction or deletion should be addressed

In France, the right of access to the Schengen Information System (SIS) could be direct for specific categories of alerts, i.e. exercised in the first instance with the data controller. The Ministry of the Interior is the competent authority for requests for access to the SIS.

In all other cases, the SIS is considered to be a file that involves State security, the defence or public safety, and therefore the right of access can only be exercised indirectly through the Commission Nationale de l'Informatique et des Libertés (CNIL).

Direct access

Ministère de l'Intérieur - Direction Générale de la Police Nationale
Place Beauvau
75008 Paris

Indirect access

Commission nationale de l'informatique et des libertés (CNIL)
Service de l'exercice des droits et des plaintes 1 (SDP1)
3, place de Fontenoy
TSA 80715
75334 Paris cedex 07
+33153732222

1.5. Functional email address

<https://www.cnil.fr/fr/demander-une-verification-sur-un-fichier-de-police-ou-de-renseignement>

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

Every data subject may send a request for the right of access to the controller, the Ministry of the Interior in Paris.

The person concerned may appoint another person (such as a lawyer) to carry out in their name and on their behalf, the exercise of the rights conferred by the GDPR and the data protection directive under the conditions described in the mandate (Decree 2019-536 of May 29, 2019 taken for the application of Law No. 78-17 of January 6, 1978, Arts. 77 and 135).

For minors and adults unable to exercise their rights on their own, it is, depending on the case, the parents, the holder(s) of parental authority or the guardian who carry out the procedure.

2.2. How the request should be submitted

According to Articles 77 and 135 of Decree No. 2019-536, the applicant must prove their identity by any means. However, when the controller has reasonable doubts as to the identity of the person, it may request any additional information that appears necessary, including, when the situation so requires, a copy of an identity document bearing the signature of the owner.

The ministry considers that it cannot allow the exercise of rights of access to its processing without

serious justification of the identity of the applicant, therefore the production of a photocopy or a scan of an identity document is systematically required.

Decree No. 2019-536 provides that the person can exercise his/her rights by using digital identity data when this data is necessary and deemed sufficient by the controller to authenticate its users. An email address does not constitute a digital identity.

The Ministry of the Interior may accept the use of substantial or high level digital identities within the meaning of European regulation eIDAS No. 910/2014 of July 23, 2014, depending on the sensitivity of the request through the use of a very secure tool, such as the digital identity card.

In accordance with the provisions of decree no. 2015-1423 of 05/11/2015 relating to exceptions to the application of the right of users to contact the administration electronically (Ministry of the Interior in this case), **requests for the right of access to the SIS can only be made by post**.

In accordance with the provisions of decree No. 2019-536 of 29 May 2019 taken for the application of the law No. 78-17 of 6 January 1978, the data controller responds to the request submitted by the interested party within two months of receipt.

The deadline is suspended when the controller requests information necessary to identify the data subject or carry out the operations requested.

2.3. Minimum information to be supplied

- The information required is as follows: surname, first names, date of birth, nationality, sex. This information is provided on the basis of the production of a valid identity document.
- The concerned person sends their request for the right of access to the controller by post. There is currently no template for access requests
- Requests for access do not have to be motivated, as well as requests for rectification or deletion of an alert, even if the information provided by the applicant on his/her situation can facilitate the processing of the request.

2.4. Documents to be supplied

- The Ministry of the Interior considers that, as the controller for the SIS, it cannot allow the exercise of access rights without serious justification of the identity of the applicant. The production of a photocopy of an identity document is systematically required as proof of identity, with a legible photograph bearing the signature of the person concerned.
- Pursuant to Articles 77 and 135 of the aforementioned decree, the request may also be presented by a person specially authorized for this purpose by the applicant, if this person proves their identity and the identity of the principal, the mandate as well as of the duration and of the precise object thereof.
- The mandate must also specify whether the proxy can be made the recipient of the response or whether it must be sent directly to the concerned person.
- The decree implementing the Data Protection Act does not mention the need for a notarial document in support of the request for the right of access.

2.5 Language regime

- In accordance with the law of 4 August 1994 on the use of the French language and in accordance with Ordinance No. 2015-1341 of 23/10/2015, referred to in Article L. 111-1 of the Code of Relations between the Public and the Administration, the use of the French language is prescribed in exchanges between the public and the administration.
- The applicants can submit their request only in French.
- The controller responds to the applicant in French.

3. Contact details of the national data protection authority

Commission nationale de l'informatique et des libertés (CNIL)

3, place de Fontenoy

TSA 80715
75334 Paris cedex 07
+33153732222
www.cnil.fr

- Right of indirect access: in certain cases, the rights can only be exercised indirectly through the CNIL.
- Right of direct access: in the absence of a response from the data controller or a response that appears to be incomplete, the rights can be exercised through the CNIL.

4. Expected outcome of requests for access. Content of the information supplied

4.1. Content of the notifications

When the request is processed by the CNIL, the Commission determines, in agreement with the data controller, which data should or should not be disclosed to the applicant with regard to the necessity to protect the purposes of the processing, State security, defence or public safety.

When the Ministry of the Interior, as data controller, objects to the disclosure of the results of the checks conducted by the CNIL, the Commission will only notify the applicant that the necessary verifications have been carried out.

The Commission's reply shall also mention the legal remedies available to the applicant. For requests relating to processing or parts of processing concerning State security, as is the case with the SIS, the mention of the legal remedies specifies that the matter may be referred to the Council of State.

If the applicant is the subject of an alert introduced by another Member State, the CNIL will seek the cooperation of the data protection agency of said State.

If the verifications give way to the suppression of the alert to which the applicant was subjected, this will be communicated to him/her providing that the data controller doesn't object to it.

If the person in charge of the treatment has given his consent, content of the notifications (whether personal data concerning the data subject is contained in the SIS, what is it, why and for what purpose it has been entered, by which authority)

When there is an SIS alert on the person concerned, the response letter indicates the reason for the search, the action to be taken and the start and end dates of the alert's validity.

4.2. Procedure to submit a complaint

5. References of the main national laws that apply

- Data Protection Act, known as loi "informatique et libertés", law No. 78-17 of 6 January 1978, modified.
- Decree No. 2019-536 of 29 May 2019 taken for the application of the data protection Act.

As mentioned above, in accordance with the law of 4 August 1994 on the use of the French language and in accordance with Ordinance No. 2015-1341 of 23 October 2015, referred to in Article L. 111-1 of the Code of Relations between the Public and the Administration, the use of the French language is prescribed in exchanges between the public and the administration.

The applicant can submit his or her request only in French.

3.10. GERMANY

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Bundeskriminalamt
BdA 4 – Petenten
65173 Wiesbaden
Tel.: +49(0)611/55-0
Fax: +49(0)611/55-12141
E-Mail: ds-potenten@bka.bund.de

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

Information from the SIS can be provided to data subjects, lawyers with power of attorney and legal guardians. Legal entities do not have the right to request information.

2.2. How the request should be submitted

The request can be submitted by e-mail or in written form. In addition, the Bundeskriminalamt (BKA, Federal Criminal Police Office) offers a contact form at the following address: https://www.bka.de/DE/KontaktAufnehmen/Kontaktinformationen/Buergerkontakt/buergerkontakt_n_ode.html

2.3. Minimum information to be supplied

Requests for information must include at least the following information: name, surname, date of birth, nationality, gender, citizenship, address.

2.4. Documents to be supplied

Requests from data subjects must also include the following documents:

- informal request for information;
- a legible copy of a valid identification document.

In case of a representation by a lawyer, the following documents are required:

- informal request for information;
- a current power of attorney mentioning the request and signed by the person concerned or a lawyer's assurance of the existence of a power of attorney mentioning the request for data information;
- legible copy of a valid identification document;
- lawyer's assurance that the client is identical with the person concerned (holder of the identity document).

2.5 Language regime

According to the national legislation "(§23 of the Verwaltungsverfahrensgesetz - Federal Law on administration procedures) the official language is German. Communication in other official languages of the EU may be accepted upon availability.

2.6. Link to website where information on how to apply for information/correction/deletion

Further information can be found on the following website:
https://www.bka.de/DE/KontaktAufnehmen/AnfragenAuskunftserteilung/AuskunftserteilungSIS/auskunftserteilungSIS_node.html

3. Contact details of the national data protection authority

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Federal Commissioner for Data Protection and Freedom of Information
Graurheindorfer Straße 153
53117 Bonn
Phone: +49 (0)228-997799-0
E-Mail: poststelle@bfdi.bund.de
De-Mail: poststelle@bfdi.de-mail.de

Website: <https://www.bfdi.bund.de/>

4. Expected outcome of requests for access. Content of the information supplied

4.1. Content of the notifications

With an information request, the person concerned or his legal representative receives information about the respective data stored in the SIS. The BKA is responsible for providing information from the SIS for Germany. If the access requirements are met, the BKA usually provides complete access to the information stored about the person concerned.

4.2. Procedure to submit a complaint

In individual cases, however, the right to information may be denied or restricted. In these cases, the following legal remedies are available:

a) Objection

Data subjects can object to rejected requests for information, rectification and deletion. The objection shall be addressed to the authority, which rejected the request.

b) Judicial protection:

If the BKA does not provide information within the deadline set in Article 12 (3) Regulation (EU) 2016/679, a lawsuit at the administrative court in Wiesbaden for the provision of the information can be filed.

c) Complaint relating to data protection law

If a request for information has been rejected, a data subject can contact the Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (for contact details, see point 3). The supervisory authority is also available for questions regarding the procedure.

5. References of the main national laws that apply

Bundesdatenschutzgesetz (BDSG) - Federal Data Protection Act (https://www.gesetze-im-internet.de/englisch_bdsg/)

3.11. GREECE

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Ministry of Citizen Protection, Section of the International Police Cooperation Division at the Hellenic Police Headquarters
3rd S.I.RE.N.E.
4 P. Kanelloupoulou Str., 10177 Athens
Telephone 210-6998263 & 210-6998262
Fax 210-6998264 & 210-6998265
Functional email address sirene@sirene.gov.gr

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

Data subjects, appointed lawyers with power of attorney, third party legally authorised, and legal guardians

2.2. How the request should be submitted

By postal mail and e-mail.

Link to online forms:

http://www.hellenicpolice.gr/index.php?option=ozi_content&lang=%27.%27&perform=view&id=26982&Itemid=898&lang=EN.

There is no deadline for the submission of an application

2.3. Minimum information to be supplied

Personal data of the applicant : name, surname, father's name, date of birth, nationality, citizenship
A model form of application can be found in:

http://www.hellenicpolice.gr/index.php?option=ozi_content&lang=%27.%27&perform=view&id=26982&Itemid=898&lang=EN (for access requests)

https://www.dpa.gr/sites/default/files/2021-05/SIS%20ce%91%ce%99%ce%a4%ce%97%ce%a3%ce%97%20%ce%94%ce%99%ce%91%ce%93%ce%a1%ce%91%ce%a6%ce%97%ce%a3%202021_final.pdf

(for correction - deletion requests)

In case of request for data correction or deletion, the justification for the request (e.g. corrections required, description of circumstances, reasoning for deletion): Data subjects are invited to provide any evidence which, in the opinion of the person concerned, should be taken into account when delivering the judgment for deletion from the relevant lists (e.g. court judgments of acquittal, residence permit for children or spouse, attestations for the submission of supporting documents for the issuance of residence permits, provided that third-country nationals are registered in the relevant lists due to a previous illegal stay).

2.4. Documents to be supplied

- proof of applicant's identity (e.g. readable copy of ID, passport, driver's licence)
- residence permit in case one has been issued already
- proof of granted power of attorney
- suitably legal authorisation document for third party representation

2.5 Language regime

The Police will normally examine requests in English in addition to Greek and reply to applicants in English if so requested.

2.6. Link to website where information on how to apply for information/correction/deletion

http://www.hellenicpolice.gr/index.php?option=ozo_content&lang=%27..%27&perform=view&id=26982&Itemid=898&lang=EN
(for access requests)
https://www.dpa.gr/en/enimerwtiko/themes/large_databases/Schengen_SISII/datasubjectsrights

3. Contact details of the national data protection authority

Hellenic Data Protection Authority
Supervisory Authority
Address: Kifissias 1-3, P.C.115 23, Athens, Greece
Telephone: +30-2106475600
Functional email address contact@dpa.gr
Website: www.dpa.gr

4. Expected outcome of requests for access. Content of the information supplied

4.1. Content of the notifications

If the alert was issued under Article 24 of SIS II Regulation, the applicant will be informed of the data relating to him.

If the alert was issued under Article 26 or Article 36 of SIS II Decision, the applicant is likely to be refused disclosure of the data. Moreover, in accordance with Article 12(5) of Law 2472/1997, the data will not be disclosed if the processing has been carried out on national security grounds or in the investigation of particularly serious offences. Where an alert under Article 26 of SIS II Decision has been issued by a foreign authority, the latter's opinion is taken into account when deciding whether to release the data to the applicant

The information released to the applicant comprises the legal basis for the alert, the date on which it was entered in the SIS II, the department which entered the data, and the length of time it is to be stored.

4.2. Procedure to submit a complaint

The national Personal Data Protection Authority checks that the SIS alert concerning the applicant is lawful and legitimate by means of examining the relevant documents supporting the decision of entering and/or maintaining the alert and will finally issue a decision on the lawfulness of the alert. Since in Greece, data subjects' rights are exercised directly before the controller i.e. the Hellenic Police, the Hellenic DPA will examine complaints on the rights of access – correction – deletion if the data subjects have addressed them before the controller and had not received a reply or the reply was unsatisfactory. Data subjects may submit a complaint in person, via postal mail and e-mail. They are also invited to fill in the relevant complaint form and submit any supporting documents for the examination of their complaint.

Details of the procedure and the relevant form can be found in:
<https://www.dpa.gr/en/individuals/complaint-to-the-hellenic-dpa>

5. References of the main national laws that apply

Law 4624/2019 - Official Gazette: (ΦΕΚ) A 137/29.08.2019, Ministerial Decree 4000/432-λα'/17.10.2012 (Official Gazette B 2805/17.10.2012) as amended by Ministerial Decree 4000/4/32-v/2017 on the criteria and the procedure for the registration and deletion of aliens to/from the National List of Unwanted Aliens

3.12. HUNGARY

1. Contact details of the body to which requests for access, correction or deletion should be addressed

SIRENE Bureau of the National Police Headquarters
H-1139 Budapest, Teve utca 4-6.
Tel: +36 1 443 5861
Fax: +36 1 443 5815
sirene@nebek.police.hu

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

Anyone who is interested in knowing whether or not their data has been recorded in the SIS, or wishes to correct or have inaccurate data deleted can submit a request. The person concerned must provide credible proof of his/her identity for authentication.

2.2. How the request should be submitted

Anyone who is interested in knowing whether or not their data has been recorded in the SIS, or wishes to correct or have inaccurate data deleted should contact any government office (<http://www.kormanyhivatal.hu/hu>), police station (<http://www.police.hu/magyarendorseg/szervezetif>) or any Hungarian Embassy or Consulate (<http://www.kormany.hu/hu/kovetsegek-konzulatusok>) and fill in a request for information form which is transferred to the SIRENE Bureau of the Hungarian National Police Headquarters.

[Form for requesting information on the basis of Art. 26 of the Act CLXXXI of 2012 on the exchange of information in the framework of the second-generation Schengen Information System](#)

2.3. Minimum information to be supplied

In the request for information form the following information are to be supplied: family name, surname, place and date of birth, gender, nationality, travel document No. (ID No), address/mailing address.

2.4. Documents to be supplied

The person concerned or his/her representative must provide credible proof of his/her identity and/or his/her authorisation.

2.5 Language regime

The request for information form is available in Hungarian and English.

2.6. Link to website where information on how to apply for information/correction/deletion

<https://www.police.hu/en/content/data-stored-in-the-sis>
<https://www.naih.hu/international-affairs-schengen-information-system>

3. Contact details of the national data protection authority

Nemzeti Adatvédelmi és Információszabadság Hatóság
(National Authority for Data Protection and Freedom of Information)

The Hungarian National Authority for Data Protection and Freedom of Information has the authority to conduct an investigation or an administrative proceedings for data protection following requests submitted to her/him according to the relevant provisions (52-61.§) of Act CXII of 2011 on Informational Self-Determination and Freedom of Information ("Privacy Act"). The Authority investigates the lawfulness of data processing and data transfer in connection with SIS II upon request or ex officio. If the data subject has doubts concerning the answer received from the SIRENE Bureau, or if no answer is received from the SIRENE Bureau, she/he may apply to the Hungarian National Authority for Data Protection and Freedom of Information.

Postal address: 1363 Budapest, Pf.: 9.
Office address: 1055 Budapest, Falk Miksa utca 9-11.
Tel. +36 (30) 683-5969
+36 (30) 549-6838
+36 (1) 391 1400
Fax: +36 (1) 391-1410
ugyfelszolgalat@naih.hu
<https://naih.hu/>

4. Expected outcome of requests for access. Content of the information supplied

4.1. Content of the notifications

The SIRENE Bureau is obliged to inform the data subject what personal data concerning the data subject is contained in the SIS, why and for what purpose it has been entered, and to whom and for what purpose it has been transferred. The SIRENE Bureau has the right to refuse the request but is obliged to inform the data subject about the fact of and the reason for denial. Information may only be denied in the interest of national security, the prevention or prosecution of crimes, the safety of the execution of sentences, and the protection of the rights of others.

4.2. Procedure to submit a complaint

If the data subject has doubts concerning the answer received from the SIRENE Bureau, or if no answer is received from the SIRENE Bureau, he/she may apply to the Hungarian National Authority for Data Protection and Freedom of Information.

5. References of the main national laws that apply

- [Act CXII of 2011 on Informational Self-Determination and Freedom of Information](#) ("Privacy Act")
- Act CLXXXI of 2012 on the exchange of information in the framework of the second-generation Schengen Information System
- Government Decree No. 15/2013. (28/I) on the detailed procedures of the exchange of information in the framework of the second-generation Schengen Information System.

The language of an administrative proceeding is Hungarian by law. However as a general rule nobody shall suffer damage or be discriminated by the fact he/she does not speak Hungarian. For the applicable rules and regulations concerning the language regime one should refer to the provisions of the [Act CL of 2016 on the Code of General Administrative Procedure](#).

3.13. ICELAND

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Applications should be addressed to the SIRENE Bureau in Iceland, which is run by the National Commissioner of the Icelandic Police (NCIP).

The NCIP's contact details are the following:

Ríkislögreglustjóri/National Commissioner of the Icelandic Police
Skúlagata 21
105 Reykjavík
ICELAND
Att. SIRENE Bureau
E-mail: rls@rls.is

2. How to make an individual request and what to include in it?

The right of access is direct, which means that data subjects have to address a request for information, correction or deletion to the SIRENE Bureau, which decides whether or not to grant access.

2.2. How the request should be submitted

Special application forms can be filled in at local police stations in Iceland or at the NCIP premises. Decisions on the release of information are taken by the SIRENE Bureau.

Access can be requested outside of Iceland. Within the Schengen Area, authorities responsible for the quality of the information registered in SIS can be contacted. Outside the Schengen Area, a request can be addressed to an embassy or a consulate of any Schengen country.

2.5 Language regime

According to Icelandic law, Icelandic is the national tongue of Iceland and an official language. When answering requests regarding SIS from foreign nationals, however, English is generally used and, if necessary, an answer will be provided for in another language which the applicant understands.

2.6. Link to website where information on how to apply for information/correction/deletion

3. Contact details of the national data protection authority

In cases where an applicant has received a standard reply: "No information is registered/it is not permitted to disclose registered information", the SIRENE Bureau must instruct the applicant that he may appeal against this decision to the DPA.

The DPA's contact details are the following:

Persónuvernd/The Data Protection Authority
Rauðarárstígur 10
105 Reykjavík
ICELAND
E-mail: postur@personusvernd.is.

4. Expected outcome of requests for access. Content of the information supplied

4.1. Content of the notifications

The SIRENE Bureau must answer all applications without undue delay and no later than a month from receipt of the request. If an applicant is registered, he will be informed of the purpose of and reasons for the registration. In cases where it is necessary to keep the information secret in order to achieve the intended aim of the entry into the information system, or in view of the interests of other persons, or when discreet surveillance is in progress, the data subject does not have the right to be informed of the recorded data. The applicant will be given the same standard reply as an applicant who is not registered, namely "No information is registered/it is not permitted to disclose registered information."

4.2. Procedure to submit a complaint

5. References of the main national laws that apply

The main national laws applying are: Act No. 51/2021 on the Schengen Information System in Iceland and Regulation No. 112/2000 on the Schengen Information System in Iceland.

3.14. IRELAND

1. Contact details of the body to which requests for access, correction or deletion should be addressed

An Garda Síochána
Data Protection Unit,
Third Floor,
89-94 Capel Street,
Dublin 1,
D01 E3C6.
Ireland

Tel. +353 (01) 666 952
DataProtection@Garda.ie

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

Data subjects, solicitors representing data subjects and the legal guardians of data subjects.

2.2. How the request should be submitted

Requests for access can be made by submitting a Data Access Request Form (F20) to the An Garda Síochána Data Protection Unit

<https://www.garda.ie/en/about-us/online-services/data-protection-foi-police-certificates/an-garda-siochana-f20-october-2019-.pdf>

2.3. Minimum information to be supplied

Full name, previous or other name(s) date of birth, current address, previous address, phone number of the applicant;

2.4. Documents to be supplied

- A request in writing must be made and signed by the applicant.
- An acceptable form of proof of identity and proof of address must accompany the Subject Access Request form:
 - o A copy of Photo ID i.e. Passport or Driving Licence and a copy of a recent Utility Bill or Government letter issued within the last six months to your current address.
- If the application is being made through a solicitor, a signed form consenting to the release of data to solicitor is required.
- Third party requests by parent/guardian requires their identification documents.

2.5 Language regime

The Data Access Request Form (F20) is requested to be completed by the data subject in English. Where necessary, additional translation services will be sought by the An Garda Síochána Data Protection Unit in relation to a request.

2.6. Link to website where information on how to apply for information/correction/deletion

<https://www.garda.ie/en/about-us/online-services/data-protection-foi-police-certificates/an-garda-siochana-f20-october-2019-.pdf>

3. Contact details of the national data protection authority

Data Protection Commission
21 Fitzwilliam Square South
Dublin 2
D02 RD28
Ireland
Telephone +353 (0)1 7650100
Functional email address info@dataprotection.ie
Website: www.dataprotection.ie
<https://forms.dataprotection.ie/contact>

4. Expected outcome of requests for access. Content of the information supplied

4.1. Content of the notifications

Following consideration of each request on a case-by-case basis, the content of the notifications may confirm/deny whether personal data concerning the data subject is contained in the SIS, a copy of the data may be supplied or restrictions invoked denying release of the data.

4.2. Procedure to submit a complaint

If the answer to a request is considered to be unsatisfactory, data subjects may lodge a complaint with the Irish data protection authority, the Data Protection Commission.

5. References of the main national laws that apply

Council Decision 2007/533/JHA

Data Protection Act 2018 (<https://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html>)

Ireland's participation in SIS II is governed by Council Decision 2007/533/JHA.

The exercise of a data subjects right's is expressly provided for in Article 58 of Council Decision 2007/533/JHA.

Sections 90-95 of the Irish Data Protection Act 2018 outline the relevant provisions regarding the data subject's rights of information (90), access (91), rectification, erasure and restriction of processing (92), the obligations of the data controller regarding communication with the data subject (93), the available restrictions for data controllers on the exercise of rights (94) and the indirect exercise of rights and verification by the Irish data protection authority, the Data Protection Commission (95).

In response to access requests specific to SIS II, the An Garda Síochána Data Protection Unit will liaise with the national SIRENE Bureau.

In response to general access requests, data subjects are provided with a disclosure detailing relevant incidents and court outcomes held on Irish police systems concerning them - this would include any incidents created as a result of actions taken by the Irish police following a relevant SIS alert (provided no restriction is applicable to the disclosure).

The vast majority of Subject Access Requests processed by the An Garda Síochána Data Protection Unit are processed within the statutory timeframe of one month provided under Section 91(2) of the Data Protection Act 2018. This timescale can be extended by a further two months owing to the volume of requests received by the controller or the complexity of the request.

Requests for rectification or erasure are managed by the Data Protection Unit in line with similar timescales as provided under Section 92 of the Data Protection Act 2018 and the provisions of Article 58 of Council Decision 2007/533/JHA (i.e. normally within one month of receipt, with a provision to extend the timescale for consideration and action but no later than three months from the date of the request).

3.15. ITALY

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Ministero dell'Interno -Dipartimento della pubblica sicurezza-Direzione centrale della polizia criminale - V Divisione - N.SIS
Via Torre di Mezzavia n. 9 00173 Roma
Telephone – not available
Fax + 39 06 46540950
dipps.dcpcsis.access@pecps.interno.it

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

Data subject, relatives (e.g. wife and husband), lawyer with power of attorney, legal guardian, third party (NGO).

2.2. How the request should be submitted

- in person, paper and/or electronic format, digitally or physically signed.
- link to online forms
- there is no deadline.

2.3. Minimum information to be supplied

- personal data of the applicant (name, surname, date of birth, nationality, gender, citizenship);
- use of model forms to exercise the rights vis-à-vis the SIS;
- in case of request for data correction or deletion, the justification for the request (e.g. corrections required, description of circumstances, reasoning for deletion) in particular by showing the previous documents on it issued by the police authorities or the decisions of the judicial authorities.

2.4. Documents to be supplied

- proof of applicant's identity (e.g. readable copy of ID, passport, residence permit, birth certificate);
- proof of granted power of attorney;
- notarial verified letter of attorney (in case of authorisation of representation by third party);.

2.5 Language regime

- For a quicker reply it is advisable that the same are written, if possible, in Italian, English, French or German. In any case, the data subject can use his own national language.

2.6. Link to website where information on how to apply for information/correction/deletion

<https://www.gpdp.it/web/guest/schengen>

3. Contact details of the national data protection authority

Garante per la Protezione dei dati personali
Supervisor Authority
Piazza Venezia 11 00187 Roma - Italy
Telephone - (+39) 06.696771
Fax - (+39) 06.69677.3785

Functional email address - protocollo@gpdp.it
Website - <https://www.gpdp.it>

4. Expected outcome of requests for access. Content of the information supplied

In the event that a satisfactory answer is not provided to the request, the interested party can make a report or a complaint, without incurring any cost, to the Italian DPA

5. References of the main national laws that apply

Personal data protection code as amended by legislative decree No 101 of 10 August 2018 containing provisions to adapt the national legal system to Regulation (EU) 2016/679, and by legislative decree No 51 of 18 May 2018 containing provisions to adapt the national legal system to directive (EU) 2016/680. There are no specific provisions in place regarding processing of SISII data for police or migration purposes; accordingly, the provisions adopted to implement the Schengen Convention by way of Law No. 388/1993, ratifying and enforcing the protocols to the Schengen Convention, continue to apply insofar as they are not incompatible with SISII Regulation (UE) 2018/1861 and Regulation (UE) 2018/1862 which will enter into force on 7 March 2023

3.16. LATVIA

1. Contact details of the body to which requests for access, correction or deletion should be addressed

State Police
SIRENE Latvia national unit
Čiekurkalna 1.linija 1, k-4 Riga, LV-1026
Ph: +371 67075212;
fax +371 67371227
e-mail: kanc@vp.gov.lv

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

In accordance with Cabinet Regulation No. 622 11 September 2007 Procedures for the Request and Issue of Information Regarding a Data Subject that is Kept in the Schengen Information System and the SIRENE Information System 3. The data subject, by submitting an application, shall confirm his or her identity by providing a personal identification document. The authorised person shall present a notably certified power of attorney that gives the right to receive information regarding the data subject or shall present a document that confirms the rights of parents, adopters, guardians or trustees. If the application is submitted electronically, the identity of the data subject shall be confirmed by a secure electronic signature.

2.2. How the request should be submitted

Requests should be submitted to the State Police or to the diplomatic and consular representations of Latvia in person or electronically, by handing in a dated and signed letter. When submitting a request in person, the data subject must prove his/her identity by presenting an identity document. If the request is submitted electronically, it should be signed with a secure electronic signature.

2.3. Minimum information to be supplied

The request should contain the surname and first name of the data subject; date of birth; personal code (if the person has one); place of birth; state of origin; type (if there is one) and number of the identity document; title of the institution that issued the document; date when the ID document was issued and its expiry date; amount of information requested (information on data subject, information on recipients of data subject information); the way the individual wants to receive the reply (in person at the State Police office or the diplomatic and consular representations of Latvia or indicate the address where the reply should be sent). The procedure is free of charge.

<https://www.dvi.gov.lv/lv/media/122/download?attachment>

2.4. Documents to be supplied

Please see 2.3.

2.5 Language regime

As for the language regime, all proceedings before Latvian authorities should be in Latvian, according to the Official Language Law of the Republic of Latvia, which also applies to rights of access to the SIS. However, the Law on Petitions (Article 7 section 1 paragraph 4) states that a petition or complaint may be unanswered if the text of the petition cannot be objectively read or understood. The SIRENE Bureau

of Latvia has stated that requests in English or Russian are also considered.

2.6. Link to website where information on how to apply for information/correction/deletion

<https://www.vp.gov.lv/lv/sengenas-informacijas-sistema>

3. Contact details of the national data protection authority

Data State Inspectorate of Latvia
National data protection authority
Elijas iela 17, Rīga, LV-1050
Phone:+371 67223131
pasts@dvi.gov.lv
<https://www.dvi.gov.lv/>

4. Expected outcome of requests for access. Content of the information supplied

4.1. Content of the notifications

The representatives of the State Police or the diplomatic and consular representations of Latvia, on receiving a request for information from a data subject, verify the identity of the data subject submitting the request and send the request to the sub-unit of the State Police – SIRENE Bureau of Latvia.

The SIRENE Bureau carries out the necessary checks on the request submitted and, within one month, provides the data subject with an answer or a refusal to provide information by sending a reply to the address or the institution indicated by the data subject - the address where the letter should be sent or to the State Police or the diplomatic and consular representations of Latvia.

Only restriction in national laws to provide answers to a data subject request is mentioned in Cabinet Regulation No. 622 11 September 2007 Procedures for the Request and Issue of Information Regarding a Data Subject that is Kept in the Schengen Information System and the SIRENE Information System 8. If the provision of the requested information is not authorised in accordance with the Law on Operation of the Schengen Information System or it is not kept in the Schengen Information System or the SIRENE information system, the answer with the following content shall be provided to the requester of the information: "There is no such information regarding you in the Schengen Information System and the SIRENE information system that you are entitled to receive on the basis of the duty to provide information specified in the Law on Operation of the Schengen Information System."

4.2. Procedure to submit a complaint

Procedure to submit a complaint is mentioned in Cabinet Regulation No. 622 11 September 2007 Procedures for the Request and Issue of Information Regarding a Data Subject that is Kept in the Schengen Information System and the SIRENE Information System 9. If it is refused to provide the requested information to the data subject or a person authorised thereof or an answer has been provided in accordance with Paragraph 8 of these Regulations, the data subject or a person authorised thereof has the right to submit a submission to the State Data Inspection regarding the necessity to examine whether the rights of the data subject specified in the Law have been followed.

5. References of the main national laws that apply

Law on operation of Schengen information system - <https://likumi.lv/ta/id/159481-sengenas-informacijas-sistemas-darbibas-likums>

Cabinet Regulation No. 622 11 September 2007 Procedures for the Request and Issue of Information Regarding a Data Subject that is Kept in the Schengen Information System and the SIRENE Information

System - <https://likumi.lv/ta/en/en/id/164148-procedures-for-the-request-and-issue-of-information-regarding-a-data-subject-that-is-kept-in-the-schengen-information-system-and-the-sirene-information-system>

3.17. LUXEMBOURG

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Requests for access should be addressed to the data protection officer of the Grand-Ducal Police of Luxembourg:

Direction Générale de la Police Grand-Ducale
A l'attention du **délégué à la protection des données**
Cité Policière Grand-Duc Henri,
B.P. 1007
L-2957 Luxembourg ,
Email : dpo@police.etat.lu

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

A request can be submitted either by the data subject or his/her attorney.

2.2. How the request should be submitted

The procedure is free of charge.

An identity verification procedure is however applied. Data subjects must proof their identity by sending to the Police a copy of an ID document. The access request procedure can be launched via letter or e-mail, both with a duly signed letter.

A request where one of these documents is missing is considered incomplete and will not be processed.

2.3. Minimum information to be supplied

- name and surname,
- nationality,
- date and place of birth,
- address.

Model letters (FR and EN) are provided on the website of the Grand Ducal Police.

In case a lawyer from abroad wishes to file a request, the following documents are required for a request to be considered complete:

- a power of attorney signed by the client and the attorney,
- a copy of an ID document of the client,
- a copy of an ID document of the attorney,
- a copy of an attorney card or equivalent.

2.4. Documents to be supplied

- a copy of an ID document of the data subject.

2.5 Language regime

The data subject may start the procedure for the right of access in one of the following languages:

- Luxembourgish;
- French;
- German;

- English.

2.6. Link to website where information on how to apply for information/correction/deletion

Data protection notice of the Grand Ducal Police containing a specific section on SIS (English version provided under the French version): <https://police.public.lu/fr/support/protection-des-donnees-a-caractere-personnel.html>

3. Contact details of the national data protection authority

Commission nationale pour la protection des données

15, boulevard du Jazz

L-4370 Belvaux

Website : <https://cnpd.public.lu/en.html>

Complaint form : <https://cnpd.public.lu/en/particuliers/faire-valoir/formulaire-plainte.html>

Telephone : (+352) 26 10 60-1

4. Expected outcome of requests for access. Content of the information supplied

4.1. Content of the notifications

The Grand Ducal Police has to provide an answer within 60 days.

If, in accordance with Article 41 (4) of Regulation 1987/2006 or Article 58 of Decision 2007/533/JHA (decision to not provide information to the data subject), and in the cases referred to in Article 12 (3) (delaying, restricting or omitting information to the data subject), Article 14 (1) (refusal or restriction of access to personal data) and Article 15 (4) (refusal of rectification or erasure of personal data) of the Act of 1 August 2018 on the protection of individuals with regard to the processing of personal data in criminal and national security matters, the Grand Ducal Police has to inform the data subjects thereof, except for those cases where even the provision of that information may be restricted for the same reasons (article 12(3), 14(2), 15(4)).

In these cases, the rights of the data subjects may be exercised through the data protection authority, which will carry out all necessary verifications. The Grand Ducal Police has to inform the data subject of the possibility to exercise his or her rights through the National Commission for Data Protection or to seek judicial remedy.

The National Commission for Data protection informs the data subject at least that it has proceeded to all necessary verifications or a review. It further informs the data subject of his or her right to seek a judicial remedy.

4.2. Procedure to submit a complaint

Should the data controller not answer within the prescribed time, or should the data subject not be satisfied with the answer received, he/she can contact the National Commission by submitting the online complaint form. The form can also be printed and send to the National Commission in paper format.

All necessary information can be found on the website of the National Commission:

<https://cnpd.public.lu/en/particuliers/faire-valoir.html>

5. References of the main national laws that apply

Law of 1 August 2018 on the protection of natural persons with regard to the processing of personal data in criminal and national security matters (implementing Directive (EU) 2016/680), in particular Articles 11, 12, 13, 14, 15, 16 and 17.

Link to the French version: <https://legilux.public.lu/eli/etat/leg/loi/2018/08/01/a689/jo>

Link to the English version: <https://cnpd.public.lu/dam-assets/fr/legislation/droit-lux/loi-police-justice-en.pdf>

Law of 1 August 2018 establishing the National Commission for Data Protection and the general rules on data protection.

Link to the French version: <https://legilux.public.lu/eli/etat/leg/loi/2018/08/01/a686/jo>

Link to the English version: <https://cnpd.public.lu/dam-assets/fr/legislation/droit-lux/Act-of-1-August-2018-on-the-organisation-of-the-National-Data-Protection-Commission-and-the-general-data-protection-framework.pdf>

Please note that only the original language version (French) is legally binding.

3.18. LIECHTENSTEIN

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Landespolizei des Fürstentums Liechtenstein (National Police)
Polizeikommando
Gewerbeweg 4
Postfach 684
9490 Vaduz
+423 236 71 11
info@landespolizei.li

2. How to make an individual request and what to include in it?

2.2. How the request should be submitted

The application for access must be addressed to the National Police in writing. In case the application is filed by a lawyer or legal guardian power of attorney resp. legal guardianship needs to be provided.

2.3. Minimum information to be supplied

The applicant must provide proof of their identity. If the application not filed in person at the National Police Force and is the applicant not a resident of Liechtenstein, the applicant must provide a certified copy of his/her passport, which must be sent per mail.

2.5 Language regime

An application can be submitted in German or English

2.6. Link to website where information on how to apply for information/correction/deletion

Information on how to apply for access/correction/deletion can be found here:
<https://www.datenschutzstelle.li/internationales/schengendublin-1>

3. Contact details of the national data protection authority

Datenschutzstelle Fürstentum Liechtenstein
Städtle 38
Postfach 684
FL-9490 Vaduz
Telefon: +423 236 60 90
E-Mail: info.dss@llv.li
www.datenschutzstelle.li

4. Expected outcome of requests for access. Content of the information supplied

4.2. Procedure to submit a complaint

Generally, a reply is given within 30 days. In case a reply cannot be given within this period the applicant has to be informed. However, an answer has to be provided no later than 60 days after filing the application. If a data subject is notified about the refusal or limitation of provision of information, the data subject may exercise their right of access via the Data Protection Authority. The National

Police shall inform the data subject about the possibility of consulting the Data Protection Authority and the available legal remedies. The Data Protection Authority further informs the data subject of the possibility of judicial remedy

5. References of the main national laws that apply

- Art. 57 ff. Data Protection Act
- Art. 34g Act concerning the National Police Force (LGBI. 1989 Nr. 48);
- Art. 29 and 30 Ordinance on the Schengen Information System (SIS) and the SIRENE Office (LGBI. 2022 Nr. 306).

3.19. LITHUANIA

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Data subjects' requests for access, correction or deletion (direct access) in Lithuania should be addressed to the Ministry of Interior of the Republic of Lithuania which is the data controller:

Ministry of the Interior of the Republic of Lithuania
Šventaragio str. 2, LT-01510 Vilnius, Lithuania
phone +370 5 271 7130
fax +370 5 271 8551
email: bendarasisd@vrm.lt

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

- data subject;
- representative of the data subject.

2.2. How the request should be submitted

The request can be submitted personally directly to the data subject or his/her representative upon arrival at the Ministry of the Interior of the Republic of Lithuania, by sending the request by mail or electronic means of communication. All requests submitted in writing, including by means of electronic communication, must be signed by the data subject who submitted the request or his/her representative. When submitting an application by means of electronic communication, a digital copy of the signed application must be submitted or the application must be signed with a qualified electronic signature that complies with the 2014 July 23 Regulation (EU) of the European Parliament and Council No. 910/2014 on electronic identification and electronic transaction reliability assurance services in the internal market, which repeals Directive 1999/93/EC. A copy of the data subject's valid passport or corresponding travel document shall be submitted together with the request submitted by mail or electronic means of communication. In the case of reasonable doubts about the identity of the data subject who submitted the request, for the purpose of identity verification, the data subject may be asked to submit a photo by post or electronic means of communication, in which the image of the data subject's face would be captured and clearly visible, together with the personal data of the data subject's valid passport or corresponding travel document a sheet with all the entries on this sheet and a photo of the person.

2.3. Minimum information to be supplied

- personal data of the applicant (surname(s) and first name(s), personal identification number (if he/she does not have a personal identification number, date of birth), place of residence, contact details (phone or email address));
- in case of request for data correction or deletion, the justification for the request (e.g. corrections required, description of circumstances, reasoning for deletion).

2.4. Documents to be supplied

- proof of applicant's identity (a copy of the data subject's valid passport or corresponding travel document);
- proof of granted power of representative.

2.5 Language regime

- Requests for access, correction or deletion must be submitted in the official language of the state (Lithuanian). The reply to the data subject is given in the official language of the state (Lithuanian).
- Requests received in any other language will be investigated according to a general procedure. If the data subject's request is in a language other than the official language of the state, it must be translated into Lithuanian. The reply will be given to the applicant in the official language of the state (Lithuanian). The language of the complaint investigation procedure is Lithuanian. Where a complaint by a data subject is lodged with the State Data Protection Inspectorate in any other language, it has to be translated into Lithuanian. The decision on the complaint is to be adopted and the reply to the complainant given in the official language of the state (Lithuanian).

2.6. Link to website where information on how to apply for information/correction/deletion

<https://www.ird.lt/en/international-cooperation-1/the-schengen-information-system>

3. Contact details of the national data protection authority

State Data Protection Inspectorate
 L. Sapiegos str. 17 , LT-10315, Vilnius, Lithuania
 phone +370 5 279 1455
 email: ada@ada.lt
 internet: www.vdai.lrv.lt

4. Expected outcome of requests for access. Content of the information supplied

The data subject has the right to obtain information on the sources and the type of personal data that has been collected on him, the purpose of their processing and the data recipients to whom the data are or have been disclosed at least during the past year.

4.2. Procedure to submit a complaint

If the data subject is not satisfied with the reply received from the data controller, or the data controller refuses to grant the data subject's request to exercise his/her right to have access to his/her personal data, to request rectification or destruction of his personal data or suspension of further processing of his personal data, or the data controller does not reply to the data subject within 30 calendar days of the date of his application, the data subject may appeal against acts (omissions) by the data controller to the State Data Protection Inspectorate. The data subject can attach documents (the data controller's answer to the data subject's request, etc.), where they exist, substantiating the facts mentioned in the data subject's complaint, in order to ensure that the complaint is investigated efficiently. After receiving the data subject's complaint, the State Data Protection Inspectorate checks the lawfulness of the personal data processing and takes a decision on the facts described in the complaint. Model letters for exercising data subjects' rights are in the following links:

- 1) https://vdai.lrv.lt/uploads/vdai/documents/files/Pavyzdinisprasymasd%C4%97teis%C4%97ssusipazinti_LT2017.docx
- 2) <https://vdai.lrv.lt/uploads/vdai/documents/files/Pavyzdinisprasymasd%C4%97teis%C4%97ssunaikintiLT2017.docx>
- 3) <https://vdai.lrv.lt/uploads/vdai/documents/files/Pavyzdinisprasymasd%C4%97teisesistaisytiLT2017.docx>
- 4) <https://vdai.lrv.lt/uploads/vdai/documents/files/RequestfordatainformationinSchengenSISII2017EN.docx>
- 5) <https://vdai.lrv.lt/uploads/vdai/documents/files/RequestfordatacorrectioninSchengenSISII2017.docx>
- 6) <https://vdai.lrv.lt/uploads/vdai/documents/files/RequestfordeletionofdatainShengenSISII2017.docx>

5. References of the main national laws that apply

- The Law on Legal Protection of Personal Data; Regulations on the Lithuanian National Schengen Information System approved by Order of 17
- September 2007 of the Minister of the Interior of the Republic of Lithuania No. 1V-324

3.20. MALTA

1. Contact details of the body to which requests for access, correction or deletion should be addressed

The Malta Police Force

Address: Police Headquarters, St Calcedonius Square, Floriana FRN 1530

Telephone: 2122 4001

Fax: N/A

Functional email address: dpu.police@gov.mt

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

Data subject, lawyer acting on behalf of the data subject and parent/legal guardian acting on behalf of a minor.

2.2. How the request should be submitted

The Malta Police Force facilitates the submissions of requests by providing a model form which can be accessed online: [https://pulizija.gov.mt/en/police-force/Pages/Schengen-Information-System-\(SIS\).aspx](https://pulizija.gov.mt/en/police-force/Pages/Schengen-Information-System-(SIS).aspx)

2.3. Minimum information to be supplied

- use of model forms to exercise the rights vis-à-vis the SIS

The data subject is requested to provide the following information when using the model form: name and surname, nationality, date of birth, ID card number, passport number and address.

- in case of request for data correction or deletion, the justification for the request (e.g. corrections required, description of circumstances, reasoning for deletion)

In the case where the data subject requests the rectification of his or her personal data, the data subject is requested to indicate which personal data are to be rectified and the reason(s) for rectification.

In the case where the data subject requests the deletion of his or her personal data, the data subject is requested to indicate which personal data are to be deleted and the reason(s) for erasure.

2.4. Documents to be supplied

The controller requests the following documents, where applicable: copy of passport, copy of the ID card and copy of the legal authorisation to represent the data subject.

2.5 Language regime

Maltese and English

2.6. Link to website where information on how to apply for information/correction/deletion

[https://pulizija.gov.mt/en/police-force/Pages/Schengen-Information-System-\(SIS\).aspx](https://pulizija.gov.mt/en/police-force/Pages/Schengen-Information-System-(SIS).aspx)

3. Contact details of the national data protection authority

Office of the Information and Data Protection Commissioner

The national supervisory authority responsible for the monitoring and enforcing the application of the data protection legislation.

Office of the Information and Data Protection Commissioner, Airways House, High Street, Sliema
SLM1549

Telephone: +356 2328 7100

Fax: N/A

Functional email address: idpc.info@idpc.org.mt

Website: <https://idpc.org.mt/>

4. Expected outcome of requests for access. Content of the information supplied

4.1. Content of the notifications

The data subjects shall have the right to obtain from the controller confirmation as to whether or not personal data concerning them are being processed, and, where that is the case, access to the personal data and the following information:

- (a) the purposes of and legal basis for the processing;
- (b) the categories of personal data concerned;
- (c) the recipients or categories of recipients to whom the personal data have been 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;
- (f) the right to lodge a complaint with the Commissioner and the contact details of the Commissioner;
- (g) communication of the personal data undergoing processing and of any available information as to their origin.

4.2. Procedure to submit a complaint

Pursuant to regulation 53(1) of Subsidiary Legislation 586.08, the data subject shall have the right to lodge a complaint with the Commissioner, if the data subject considers that the processing of personal data relating to him or her infringes the data protection regulations.

The Commissioner facilitates the submissions of complaints by providing a complaint submissions form which can be completed electronically on its website: <https://idpc.org.mt/raise-a-concern/>

This, however, does not exclude other means of communication insofar as the complaint is made in writing.

5. References of the main national laws that apply

Part III of the Data Protection (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) Regulations, Subsidiary Legislation 586.08 sets forth the rights of the data subjects.

In terms of regulation 15(1) of Subsidiary Legislation 586.08, the data subjects' rights may be restricted, wholly or partly, and for as long as such a partial and complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned, for any of the following reasons:

- (a) avoid obstructing official or legal inquiries, investigations or procedures;

- (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- (c) protect public security;
- (d) protect national security;
- (e) protect the rights and freedoms of others.

Regulation 15(2) of Subsidiary Legislation 586.08 states that the controller shall inform the data subject, without undue delay, and in no later than forty days from receiving the request, in writing of any refusal or restriction of access and of the reasons for the refusal of the restriction.

The languages of the requests and the replies should be in Maltese and English. Article 5(2) of the Constitution of Malta provides that "any person may address the Administration in any of the official languages and the reply of the Administration thereto shall be in such language".

3.21. NETHERLANDS

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Dutch National Police - Central Unit
Privacy Desk
PO Box 100
3970 AC Driebergen
Tel: +31 618 144 712
e-mail: jz.le@politie.nl

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

Any individual or his or her (legal) representative or legal guardian (in case of a minor under the age of 16 or persons under guardianship) can submit an individual request.

2.2. How the request should be submitted

A request must be submitted in writing, or by completing the designated form on www.politie.nl via <https://www.politie.nl/en/contact/forms/schengen-request-form.html?sid=ac78a8bc-d5f8-4e56-ab3b-aa85818fd529>

Requests are made free of charge.

Once access to data has been provided, a subsequent request may be submitted for data to be rectified or erased. The applicant will be informed within 6 weeks after submitting the rectification or erasure request.

2.3. Minimum information to be supplied

Upon receiving a request for access, the Data Protection Officer must ensure that the identity of the data subject is properly established. If the Data Protection Officer has reason to doubt the identity of the data subject, additional information necessary to confirm the identity of the data subject may be requested.

2.4. Documents to be supplied

All requests must be accompanied by a valid proof of identity and the applicant's signature. A copy of the identity document must be provided and – where applicable – proof of legal authorisation to represent the applicant. Requests on behalf of minors or persons under guardianship must also be accompanied by proof of authorisation.

2.5 Language regime

- Requests may be submitted preferably in Dutch or English, but will also be accepted in French, German or Spanish.
- Requests will be replied to in Dutch, unless the request is made in English, French, German or Spanish. A reply in that case will be in English. Applicants using another language than Dutch should take additional time for translation into account.

2.6. Link to website where information on how to apply for information/correction/deletion

Schengen | politie.nl ; <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/politie-justitie/europese-informatiesystemen>

3. Contact details of the national data protection authority

Dutch Data Protection Authority (Autoriteit Persoonsgegevens)
PO Box 93374
2509 AJ DEN HAAG
The Netherlands
Tel. +31-70-8888500
Fax +31-70-8888501
e-mail info@autoriteitpersoonsgegevens.nl
website www.autoriteitpersoonsgegevens.nl

The Dutch Data Protection Authority is the national supervisory authority responsible for supervision of the processing of personal data in N.SIS. The data subject may request the Dutch Data Protection Authority for mediation or advice in case of a dispute with the controller regarding the processing of a request for access to data, or a request for completion, rectification or erasure. An application must be submitted within 6 weeks of receipt of the controller's decision. The Dutch Data Protection Authority can also handle complaints lodged by a data subject, or by a body, organisation or association representing the data subject.

4. Expected outcome of requests for access. Content of the information supplied

4.1. Content of the notifications

The data subject has the right to obtain from the controller confirmation as to whether or not personal data relating to them are being processed and, where that is the case, to access such personal data and to obtain information on:

- a. the purposes and the legal basis of the processing;
- b. the categories of police data concerned;
- c. whether the data concerning that person have been provided throughout a period of four years prior to the request and on the recipients or categories of recipients to whom the data have been disclosed, in particular recipients in third countries or international organisations;
- d. the envisaged period of storage or, if that is not possible, the criteria for determining that period;
- e. the right to request rectification, destruction or restriction of the processing of data relating to them;
- f. the right to lodge a complaint with the Dutch Data Protection Authority, and the contact details of the authority;
- g. the origin, to the extent available, of the processing of the data relating to them.

Within 6 weeks after submitting the request a reply must be communicated to the applicant.

4.2. Procedure to submit a complaint

If a data subject does not agree with the reply to his or her request for access, rectification or erasure, an appeal can be lodged with the administrative section of the District Court. Under Dutch administrative law, an appeal must be submitted within 6 weeks after the reply was sent to the applicant.

The data subject may also request the Dutch Data Protection Authority for mediation or advice in case of a dispute with the controller regarding the processing of his or her request for access, rectification or erasure. An application must be submitted within 6 weeks of receipt of the controller's decision.

If mediation by the Dutch Data Protection Authority has failed, an appeal may be lodged with the District Court to consider the case as it finds appropriate. Such an appeal may be filed after the interested party

has received notification from the Dutch Data Protection Authority that the mediation case is closed, but in any event no later than 6 weeks after this notification. Without prejudice to existing means of redress, every data subject has the right to file a complaint with the Data Protection Authority if the data subject is of the opinion that the processing of personal data concerning them is unlawful. Complaints can be submitted in writing or by using the designated online form [Meldingsformulier klachten | Autoriteit Persoonsgegevens](#)

5. References of the main national laws that apply

The Police Data Act (Wet politiegegevens) and the Police Data Decree (Besluit politiegegevens) are applicable to personal data in case of law enforcement related SIS alerts. The GDPR is applicable to personal date in case of migration related SIS alerts.

The Dutch General Administrative Law Act (Algemene wet bestuursrecht) provides for administrative procedural rules with regard to decisions of administrative bodies and appeal procedures.

A request for access, rectification or deletion may be refused to the extent that this constitutes a necessary and proportionate measure, to avoid obstructing legal inquiries, investigations or procedures; to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or the execution of criminal penalties; to protect public security or to protect the rights and freedoms of third parties.

3.22. NORWAY

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Kripo
(National Criminal Investigation Service - NCIS)
PO Box 2094 Vika
NO-0125 OSLO
Tel.: +47 23 20 80 00
Fax: +47 23 20 88 80
E-mail: kripo@politiet.no
Internet: www.politiet.no

2. How to make an individual request and what to include in it?

Applications for access must be made in writing and signed. A proof of identity must be attached. A written reply must be given without undue delay and no later than 30 days from receipt of the request.

2.1. Who can submit a request

A data subject or a person who presumes to be registered can submit a request, as well as a lawyer or other representative or legal guardian.

If the person listed in the database is younger than 15 years of age, the request must be signed by a parent or legal guardian. From the age of 15, listed persons can request access themselves under the Police Databases Act. Parents/legal guardians can, on their own initiative, request access to information about the listed person (the minor) until the minor reaches the age of 18. The minor should be informed of such requests.

Legal representatives or anyone requesting access on behalf of somebody else, must present a valid letter of authority.

2.2. How the request should be submitted

A request should be submitted in writing, either on paper or in an electronic format.

Link to online form: [request-for-access-to-information-in-the-schengen-information-system-sis.pdf
\(politiet.no\)](http://request-for-access-to-information-in-the-schengen-information-system-sis.pdf_(politiet.no))

2.3. Minimum information to be supplied

- Name, address, postal code, city, country, date of birth, telephone number, e-mail address.
- Description of the information you request access to, seek to have corrected or deleted. In case of request for data correction or deletion, the justification of the request: e.g. the corrections required, description of circumstances, reasoning for the correction or deletion.
- Proof of applicant's identity.
- If you have a Norwegian national identity number or a central immigration system number, please state this.
- If you are represented by an agent, legal representative or other, please present a valid letter of authority.

- The following are considered valid proof of identity:
- Valid passport (not emergency passport)
 - Norwegian bank card with a photo
 - Norwegian driving licence (not older versions – “green driving licence”)
 - Nordic driving licence of EU/EEA standard
 - The Ministry of Defence's ID card (from 2004)
 - Valid Norway Post ID card issued after 1 October 1994
 - National ID card issued in the EEA
 - Asylum application registration card with signature and place of birth
 - Norwegian refugee travel document (green passport)
 - Norwegian immigrant's passport (blue passport)

2.4. Documents to be supplied

- Proof of applicant's identity.
- Form for request provided by NCIS.
- If relevant, valid letter of authority.

2.5 Language regime

You may submit your request in English, Norwegian, one of the Sami languages, Swedish or Danish. The reply from Norwegian authorities will be in English or in Norwegian.

2.6. Link to website where information on how to apply for information/correction/deletion

Access to information in the Schengen Information system – Politiet.no

3. Contact details of the national data protection authority

Datatilsynet
PO Box 458 Sentrum
NO-0105 OSLO
Tel.: +47 22 39 69 00
Fax: + 47 22 42 23 50
E-mail: postkasse@datatilsynet.no
Internet: www.datatilsynet.no/en

4. Expected outcome of requests for access. Content of the information supplied

In case there is an alert in the SIS, and as long as the information can be communicated to the data subject, the following information is provided to the applicant: kind of alert and for what purpose; Member State that introduced the alert; date of creation of the alert; other personal data processed in the SIS, including photograph, if applicable.

If the request (for data correction or deletion) is denied, the applicant is informed about the possibility to challenge this decision in the court.

4.2. Procedure to submit a complaint

A complaint to the Norwegian Data Protection Authority should be made in writing, either on paper or in an electronic format. There is no deadline to complain to the Norwegian Data Protection Authority.

Link to information on how to complain to the Norwegian Data Protection Authority:
<https://www.datatilsynet.no/en/about-us/contact-us/how-to-complain-to-the-norwegian-dpa/>

If your request has been denied by Norwegian authorities or your complaint has been dismissed by the Norwegian Data Protection Authority, you may challenge this decision before the courts of Norway.

Compensation

You may be entitled to compensation if you have suffered some harm because of the information recorded unlawfully in the database, or if information is used in a way that breaks the SIS rules. Please see the Norwegian Act relating to the Schengen Information System no. 6 of 18 February 2022 Section 19 and Section 20 and Regulation relating to the Schengen Information System no. 1194 of 26 June 2022 Section 2 and Section 3.

You must claim compensation no later than one year after you found out what information had been recorded. You can send your claim for compensation to Norway's NCIS or to the authority that decided the information should be recorded.

You may complain to the National Police Directorate or the Ministry of Justice and Public Security if your claim for compensation have been rejected.

5. References of the main national laws that apply

- Act relating to the Schengen Information System no. 66 of 16 July 1999 (LOV-1999-07-16-66).
Link to Norwegian text: <https://lovdata.no/lov/1999-07-16-66>
- Regulation relating to the Schengen Information System no. 1194 of 26 June 2022 (FOR-2022-06-26-1194). Link to Norwegian text: <https://lovdata.no/forskrift/2022-06-26-1194>

3.23. POLAND

1. Contact details of the body to which requests for access, correction or deletion should be addressed

1.1. Official name of the body to which a request for access should be addressed

Komendant Główny Policji (en. Commander-in-Chief of the Police)

1.2. Address

Central Technical Authority of the National IT System (CTA NITS)

National Police Headquarters

148/150 Puławska St.

02-624 Warsaw

Poland

1.3. Telephone

+ 48 47 72 148 79

+ 48 47 72 131 45

1.4. Fax

+48 47 72 129 21

1.5. Functional email address

The National Police Headquarters has launched an Electronic Inbox on the ePUAP platform. It enables the receipt and handling of electronic documents signed with a qualified electronic signature. Please note that in order to submit an application to the National Police Headquarters, it is necessary to have a free user account on the ePUAP platform. Electronic Platform of Public Administration Services (ePUAP) is a Polish nationwide platform for communication of citizens with public administrations in a uniform and standardized way. Built as part of the ePUAP-WKP project (State Informatization Plan). Service providers are public administration units and public institutions (especially entities that perform tasks commissioned by the state). Currently all administration services are available in Polish only.

<http://bip.kgp.policja.gov.pl/kgp/elektroniczna-skrzynka/11424,Elektroniczna-skrzynka-podawcza.html>

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

Every person has the right to:

- access to own personal data
- rectification of inaccurate own personal data
- erasure of personal data unlawfully processed

- file a complaint to the President of the Personal Data Protection Office

A person may be represented by a proxy, unless the nature of the act requires his / her personal action, in accordance with art. 32 of the Act of 14 June 1960, the Polish Administrative Code (Journal of Laws of 2022, item 2000, as amended).

Rules of giving legal proxy are set in art. 33 the Polish Administrative Code, i.e.:

- the proxy of a party can be natural person having legal capacity;
- the proxy should be submitted in writing;
- the proxy attaches to the file an original or officially certified copy of the proxy.

A lawyer or a legal/tax advisor and patent agent can certify a copy of a proxy given to them

2.2. How the request should be submitted

The application to Central Technical Authority of the National IT System (CTA NITS) - The Commander in Chief of the Police can be directed to:

- By post:

Central Technical Authority of the National IT System (CTA NITS)

National Police Headquarters

148/150 Puławska St.

02-624 Warsaw

Poland

- via an electronic inbox available at: http://bip.kgp.policja.gov.pl/kgp/elektroniczna-skrzynka/11424_Elektroniczna-skrzynka-podawcza.html

Schengen-related requests received (also by e-mail) by the Protection Personal Data Protection Office - the national data protection authority - are forwarded, according to jurisdiction, to the National Police Headquarters.

2.3. Minimum information to be supplied

For this purpose, a written application should be submitted in Polish, which should obligatorily include:

- a) name(s) and surname of the applicant;
- b) citizenship;
- c) date and place of birth (city and country);
- d) address for return correspondence (country, city, postal code, poviat/area, voivodeship/district, street and house/apartment number) - in the case of an application sent by post;
- e) the subject of the application;
- f) handwritten signature of the person submitting the application.

Additionally, in order to unambiguously identify the data, the applicant may provide in the application:

- a) previous/family name;
- b) PESEL number (if the person has it);
- c) sex;
- d) place of residence (country, city, postal code, poviat/area, voivodeship/district, street and

- house/apartament numer);
- e) attach a photo copy of the page of the identity document containing personal data.

In case of doubts as to the identity of the person who submitted the application, the administrator may request additional information necessary to confirm the person's identity (Article 28 Act *d.p.c.c.* and Article 12 paragraph 6 *GDPR*).

The form which can be used to submit an application is available at:
<https://www.policja.pl/pol/sirene/prawo-osob-do-informac/76188/The-right-of-data-subjects-to-information.html>.

2.4. Documents to be supplied

- Written application.
- A copy of a valid identity document as defined by the national law of a Schengen State (passport/ID card/driving licence (other valid identity document));
- An original or officially certified copy of the proxy (in case of authorisation of representation by third party).

2.5 Language regime

In Poland, the official language is Polish, therefore all the applications must be submitted in Polish.

2.6. Link to website where information on how to apply for information/correction/deletion

- <https://www.policja.pl/pol/sirene/prawo-osob-do-informac/76188/The-right-of-data-subjects-to-information.html>
- <https://uodo.gov.pl/pl/479/2064>

3. Contact details of the national data protection authority

3.1 Official name of the national data protection authority

Urząd Ochrony Danych Osobowych (en. Personal Data Protection Office)

3.2 Role

In order to provide an adequate level of legal protection for persons whose data is stored in the Schengen Information System, Personal Data Protection Office supervises whether the use of data violates the rights of data subjects. This supervision is exercised in accordance with the laws on personal data protection.

Any person whose data are processed in the Schengen Information System, is entitled to submit a complaint to the President of the Personal Data Protection Office in relation to the implementation of the provisions on the protection of personal data.

3.3 Address of the responsible body

Personal Data Protection Office
2 Stawki St.
00-193 Warsaw

Poland

3.4 Telephone

Telephone: +48 22 531 03 00

3.5 Fax

Fax: +48 22 531 03 01

3.6 Functional email address

kancelaria@uodo.gov.pl

3.7 Website:

<http://www.uodo.gov.pl>

4. Expected outcome of requests for access. Content of the information supplied

4.1. Content of the notifications

The data subjects rights are exercised in the Republic of Poland on the basis of the provisions of the GDPR or on the basis of the Act of 14 December 2018 on the protection of Personal Data processing with regard of prevention and combating crime, (depending on the purpose of data processing, e.g. category of alerts).

According to the Art. 15 (1) of the GDPR 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.

According to the Act of 14 December 2018 on the protection of Personal Data processing with regard of prevention and combating crime the data subject shall have the right, on his request, to obtain from the controller whether his or her data are processed or, where they have been processed, the right to be informed of:

- 1) the purpose of and legal basis for their processing;
- 2) the categories of personal data and of the data which are processed;
- 3) the recipients or categories of recipients to whom the personal data have been disclosed, in particular recipients in third countries or international organisations;
- 4) the period during which the personal data will be stored or, where that is not possible, the criteria used to determine that period;
- 5) the possibility of applying to the controller for the rectification or erasure of personal data or restricting the processing of personal data relating to that controller;
- 6) the right to submit to the President of the Office or to any other supervisory authority on the basis of a separate complaint, in the event of a breach of the rights of the person as a result of the processing of his or her personal data, and of the data of the competent authority of the President or of the other supervisory authority;
- 7) source of data.

According to the Art. 23 of the Act of 14 December 2018 on the protection of Personal Data processing with regard of prevention and combating crime the data subject shall, at his or her request, be entitled to have access to his or her own personal data. Having regard to the request for access to personal data, the controller shall make available or provide to the applicant a copy of, or a copy of such data, in an accessible form. The controller shall inform the data subject of the reasons for the refusal or restriction of access and of the possibility to lodge a complaint with the President of the Office in the event of a breach of the rights of the person as a result of the processing of his or her personal data. The controller shall document the factual or legal reasons for refusal or restriction of access. The President of the Office shall, on his request, be made available to this information.

4.2. Procedure to submit a complaint

Anyone who believes that his or her personal data protection rights have not been respected may lodge a complaint against the controller with the President of the Personal Data Protection Office. Complaints may be submitted in written or electronic form. The complaint shall be sent by electronic means through the Electronic Inbox of the President of the Office, after completing the FORM – i.e. "General letter to a public body" available on ePUAP2 portal. With regard to Schengen-related issues, the DPA handles complaints that are lodged by e-mail.

Each complaint must contain:

- name and surname and address of residence;
- indication of the entity against which the complaint is lodged (name/name and surname, and address of the seat/residence);
- a detailed description of the violation;

- your request, i.e. indication of what action you expect from the Personal Data Protection Office (e.g. erasure of data, fulfilment of the information obligation, rectification of data, limitation of data processing, etc.);
- handwritten signature;

It is important to attach evidence confirming the controller's incorrect action (e.g. correspondence with the controller, contracts, certificates). This will make it easier for the Office's staff to assess the case. Complaints which do not contain the name and address will not be further considered due to the impossibility of contacting the complainant.

Details of how to lodge a complaint to the President of the Personal Data Protection Office are available at: <https://uodo.gov.pl/en/559/941>.

5. References of the main national laws that apply

- **Act of 24 August 2007 on the participation of the Republic of Poland in the Schengen Information System and the Visa Information System (OJ 2021.1041 of 09.06.2021)**

The Act defines the principles and method of implementation of the Republic of Poland's participation in the Schengen Information System and the Visa Information System, including the obligations and rights of the authorities to make entries and consult data contained in the Schengen Information System and the Visa Information System through the National Information System.

- **Act of 10 May 2018 on the Protection of Personal Data (OJ 2019.1781 of 19.09.2019)**
This Act applies to the protection of natural persons in connection with processing of personal data within the scope defined in Article 2 and Article 3 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Official Journal of the European Union L 119 of 04.05.2016, p. 1), hereinafter referred to as "Regulation 2016/679".
- **Act of 14 December 2018 on the protection of Personal Data processing with regard of prevention and combating crime (OJ 2019.125 of 22.01.2019)**

The Act sets out:

- 1) the terms and conditions for the protection of personal data processed by competent authorities for the purpose of identifying, tracing, detecting and combating criminal offences, including threats to security and public order, and the exercise of pre-trial detention, penalties, disciplinary sanctions and coercive measures for deprivation of liberty;
- 2) rights of data subject processed by the competent authorities for the purposes referred to in point 1 and their remedies;
- 3) the method of keeping of the supervision of the protection of personal data processed by the competent authorities for the purposes referred to in point 1, excluding data processed by the prosecution and the courts;

- 4) the tasks of the supervisory authority and the form and manner of their implementation
- 5) the obligations of the controller and of the processor and of the data protection officer and the procedure for its designation;
- 6) preservation of personal data;
- 7) procedures for cooperation between supervisory authorities in other Member States of the European Union;
- 8) criminal liability for failure to comply with the provisions of this Act.

- **Act of 14 June 1960, Code of Administrative Procedure (OJ 2022.2000 of 27.09.2022)**

The Code of Administrative Procedure shall govern proceedings: 1) before public administration bodies in cases that are within the jurisdiction of such bodies and individually decided by way of administrative decision.

- **Act of 7 October 1999 on the Polish Language (OJ 2021.672 of 12.04.2021)**

The provisions of the Act concern use of the Polish language in the implementation of public tasks.

3.24. PORTUGAL

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Gabinete Nacional SIRENE / SIRENE Bureau
Av. Defensores de Chaves, 6, 1049-063 Lisboa, Portugal
+351. 217 822 000
sirene.portugal@sef.pt

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

- Any individual;
- The applicant can be represented by a lawyer with powers of attorney, which should expressly mention in the mandate the exercise of the data protection rights;
- In case of a minor, the exercise of the rights can be performed by the respective legal representative.

2.2. How the request should be submitted

- in person;
- by post mail. (Not admissible requests by email).

2.3. Minimum information to be supplied

- Personal data of the applicant (name, surname, nationality, date of birth, place and country of birth; parents' name and surname, if applicable; passport or ID card number, date of issuance and expiry, issuer body; number of residence permit, issuance and validity date)
- Contact details (postal address, telephone, email)
- use of model forms to exercise the rights vis-à-vis the SIS, available for download in the organisation website in PT and EN versions.
- in case of request for data correction or deletion, the justification for the request (e.g. corrections required, description of circumstances, reasoning for deletion)

2.4. Documents to be supplied

- readable certified copy of ID or passport, and of residence permit, if applicable
- proof of granted power of attorney, duly signed by the applicant (original)
- in case of minors, proof of legal representation by parents or others holding parental responsibility (original or certified copy).

2.5 Language regime

- what language(s) can be used to submit the request: Portuguese. (The model forms are available in English to assist fulfilment of the request).
- what language is used to reply to the applicant: Portuguese.

2.6. Link to website where information on how to apply for information/correction/deletion

PT version: <https://www.puc-spoc.pt/direitos-schengen>

EN version: <https://www.puc-spoc.pt/en/schengen-rights>

3. Contact details of the national data protection authority

Comissão Nacional de Proteção de Dados (CNPD)
Av. D. Carlos I, 134, 1.º, 1200-851 Lisboa, Portugal
Tel. +351. 213.928.400
Fax: +351.213.976.832
geral@cnpd.pt
<https://www.cnpd.pt/>

4. Expected outcome of requests for access. Content of the information supplied

4.1. Content of the notifications

In case there is an alert in the SIS, and as long as the information can be communicated to the data subject, the following information is provided to the applicant: kind of alert and for what purpose; Member State that introduced the alert; date of creation of the alert and data of its actual validity; other personal data processed in the SIS, including photograph and fingerprints, if applicable.

Depending on the specifics of the request and of the case, further information can be communicated to the applicant (e.g. authority requesting the creation of the alert; facts and legal reasoning for the alert; ongoing consultations between competent authorities of Member States).

If the request (for data correction or deletion) is denied, the applicant is informed about the possibility to challenge this decision in the court.

4.2. Procedure to submit a complaint

Complaints should be submitted through a specific form available in the CNPD's website.
<https://www.cnpd.pt/cidadaos/participacoes/geral/>

5. References of the main national laws that apply

- [Decree-Law 122/2021](#), of 30 December
- Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR)
- [Law 59/2019](#), of 8 August .

3.25. ROMANIA

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Centre for International Police Cooperation - SIRENE Bureau
1-5 Calea 13 Septembrie, Bucharest, 5th District
Tel: +40 21 315 96 26; +40 21 314 05 40
Fax: +40 21 314 12 66; +40 21 312 36 00
ccpi@mai.gov.ro

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

- data subject, lawyer with power of attorney, legal guardian

Persons whose personal data are collected, held or otherwise processed in the SIS II are entitled to rights of access, correction of inaccurate data and deletion of unlawfully stored data.

2.2. How the request should be submitted

- by regular post, by email.

2.3. Minimum information to be supplied

- personal data of the applicant (name, surname, date of birth, nationality, gender, citizenship);
- in case of request for data correction or deletion, the justification for the request (e.g. corrections required, description of circumstances, reasoning for deletion)

2.4. Documents to be supplied

- proof of granted power of attorney
- notarial verified letter of attorney (in case of authorisation of representation by third party)

2.5 Language regime

- the request can be submitted in Romanian or English
- the reply will be in Romanian or English, depending on the language used for submitting the request

2.6. Link to website where information on how to apply for information/correction/deletion

<https://www.dataprotection.ro/index.jsp?page=schengen&lang=en>

3. Contact details of the national data protection authority

Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)
28-30 Gheorghe Magheru Blvd, 1st District, Bucharest
Tel: +40.318.059.211
Fax: +40.318.059.602
anspdcp@dataprotection.ro
www.dataprotection.ro

Pursuant to Article 64 of Law no. 141/2010, republished, the legality of the processing of personal data in N.SIS on the territory of Romania and the transmission of this data abroad, as well as the exchange and further processing of additional information are monitored and subject to the control of the National Supervisory Authority for Personal Data Processing (ANSPDCP).

In case the data subject does not receive a reply to his/her request for exercising the rights or is not satisfied with the answer received, he/she has the right to submit a complaint to ANSPDCP.

4. Expected outcome of requests for access. Content of the information supplied

4.2. Procedure to submit a complaint

Right of access

The right of access is the possibility for anyone who so requests to have knowledge of the information relating to him or her stored in a data file as referred to in national law. This is a fundamental principle of data protection which enables data subjects to exercise control over personal data kept by third parties. This right is expressly provided for in Article 53 of Regulation (EU) 2018/1861 and in Article 67 of Regulation (EU) 2018/1862.

The right of access is exercised in accordance with Law no. 141/2010, republished. Thus, pursuant to Article 62 of Law no. 141/2010, republished, the requests of the data subjects in the context of personal data processed in the NISA or the SIS can be submitted only to the national SIRENE Bureau which will communicate the answer to the applicant as soon as possible but no later than 60 days after the receipt of the request.

The requests may be submitted to the national SIRENE Bureau or to any data controller within the Minister of Internal Affairs or its structures, which sends the request to the national SIRENE Bureau within 5 days from its submission.

In the case of alerts entered in the SIS by another Member State, the requests of the persons are answered by the national SIRENE Bureau only with the consent of the Member State that entered the alert. The national SIRENE Bureau requests the consent through the exchange of supplementary information.

The data subject shall not be communicated information regarding personal data processed in SIS as long it is necessary for performing the activities on the basis of the alert or the objective of the alert or for protecting the rights and freedom of other persons.

Right to rectification and deletion of data

Besides the right of access, there are also the right to obtain the correction of personal data factually inaccurate or incomplete or the right to ask for deletion of personal data unlawfully stored (Article 53 of Regulation (EU) 2018/1861 and Article 67 of Regulation (EU) 2018/1862).

Under the Schengen legal framework only the Member State responsible for issuing an alert in the SIS may alter or delete it (See Article 44(3) of Regulation (EU) 2018/1861 and Article 59(3) of Regulation (EU) 2018/1862).

The right of rectification and deletion of data is exercised in accordance with Law no. 141/2010, republished. Thus, pursuant to Article 62 of Law no. 141/2010, republished, the requests of the data subjects in the context of personal data processed in the NISA or the SIS can be submitted only to the national SIRENE Bureau which will communicate the answer to the applicant as soon as possible but no later than 90 days after the receipt of the request.

The requests may be submitted to the national SIRENE Bureau or to any data controller within the

Minister of Internal Affairs or its structures, which sends the request to the national SIRENE Bureau within 5 days from its submission.

If the request is submitted in a Member State that did not issue the alert, the competent authorities of the Members States concerned cooperate to handle the case, by exchanging information and making the necessary verifications.

5. References of the main national laws that apply

- Law no. 141/2010 on the setting up, organisation and functioning of the National Information System for Alerts and participation of Romania to the Schengen Information System, republished
- Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals
- Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006
- Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU

3.26. SLOVAK REPUBLIC

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Ministerstvo vnútra Slovenskej republiky (Ministry of Interior of the SR)
Prezídium Policajného zboru
Úrad medzinárodnej policajnej spolupráce
Národná ústredňa SIRENE
Pribinova 2
812 72 Bratislava
Slovenská republika
sirene@minv.sk

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

The request can submit any individual or deputy of the individual (a person authorised by data subject with the procuration).

2.2. How the request should be submitted

Written request shall be submitted

- in person, by post or electronically signed with electronic signature to the address of the Ministry of Interior of SR
- by email,
- by standard application form available on the website of the Ministry of Interior of SR

In Slovak

<https://www.minv.sk/?Prava>

In English

<https://www.minv.sk/?Data-Subjects-Rights>

Deadline: The controller shall provide information on action taken on a request 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.

2.3. Minimum information to be supplied

The data subject is obliged to provide his/ her personal data (name, surname, address of permanent residence, place and full date of birth and nationality) as well as a copy of his/her ID card or passport for the purpose of proving his/her identity. If data subject is not a Slovak national, a colour copy (scan) of another document proving name and surname or changes of name/surname during your entire life (birth certificate, marriage certificate). Delivery address or email - depending on by which means the data subject wants an answer.

Forms:

- [Request for provision of information on personal data processed in the Schengen Information System_2018 \(RTF, 74 kB\)](#)
- [Request for rectification of incorrect or outdated personal data processed in the Schengen Information System \(RTF, 75 kB\)](#)

- [Request for destruction of illegally processed personal data in the Schengen Information System \(RTF, 74 kB\)](#)

In case of request for data correction or deletion, the applicants are informed to justify their request (identification of the object and proving relation to it).

2.4. Documents to be supplied

A copy of the applicant ID card or passport for the purpose of proving his/her identity. If data subject is not a Slovak national, a colour copy (scan) of another document proving name and surname or changes of name/surname during your entire life (birth certificate, marriage certificate). Document stating parental relationship (concerning request for a child).

If request is sent through a person authorised by data subject, it is required to attach the copy of the procuration to the request translated into English or Slovak language and certified by a notary.

2.5 Language regime

Slovak or English.

2.6. Link to website where information on how to apply for information/correction/deletion

In Slovak

<https://www.minv.sk/?Prava>

In English

<https://www.minv.sk/?Data-Subjects-Rights>

3. Contact details of the national data protection authority

Úrad na ochranu osobných údajov Slovenskej republiky
(Office for Personal Data Protection of the Slovak Republic, "Office")
Hraničná 12, 827 07 Bratislava 27, Slovenská republika (Slovak Republic)
Tel: +421 2 3231 3214
Fax: +421 2 3231 3234
statny.dozor@pdp.gov.sk
<https://dataprotection.gov.sk/uouu>

The Office is a state administration body with national jurisdiction over the territory of the Slovak Republic that participates in the protection of fundamental rights of natural persons in relation to processing of personal data and executes data protection supervision, including supervision of personal data protection by competent authorities for performance of the task for the purposes of criminal proceedings

4. Expected outcome of requests for access. Content of the information supplied

4.1. Content of the notifications

The notification contains information about the data subject, what data, why and for what purpose and also by whom it has been entered. If the record contains photographs or dactyloscopic data of the person, data subject is informed that the record also contains this data. The notification contains also information that the data is accurate, actual and processed in compliance with the applicable laws. It contains also information on lodging the complaint with regard to data protection.

4.2. Procedure to submit a complaint

The right to lodge a complaint referred to as a request for verification of processing shall apply to the Office if the data subject (individual) considers that his or her data is being processed unlawfully in the relevant national component of the SIS. The Office is competent to review personal data processing within the national part of the SIS in case where there is suspicion of an unlawful procedure or a satisfactory response was not provided. According to the sec. 100 para. 3 of the Act. No. 18/2018 Coll. the complaint shall contain:

- **the name, surname, correspondence address and signature of the complainant,**
- **identification of the entity against which the complaint is addressed,** name, surname, permanent residency or organization name, headquarter and identification number if such number was assigned,
- **the subject of the complaint,** identifying the rights that might have been infringed during personal data processing,
- **evidence supporting the arguments stated in the complaint,**
- **copy of document or other type of evidence demonstrating the exercise of a right pursuant to second title of second chapter of the Act. No. 18/2018 Coll. or the Regulation 2016/679** if you have exercised such right, **or the reasons worth special consideration** if you have not exercise such right.

The complaint shall be submitted in Slovak language (the official translation is not required). The template of the complaint can be found [here](#). **This template serves only for the information about the content requirements of the complaint.** In accordance with the Act No. 270/1995 Coll. on the State Language of the Slovak Republic the public authorities and the natural persons are obliged to use the state language – Slovak in the official communication. The proceeding is performed and the decisions are issued exclusively in Slovak language.

5. References of the main national laws that apply

- Act No. 18/2018 Coll. on personal data protection and amending and supplementing certain Acts
- Civil Code No. 64/1964 Coll. (section 22 – 33b provisions on representation)

3.27. SLOVENIA

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Policija, Ministrstvo za notranje zadeve
Štefanova 2
1501 Ljubljana
Slovenia
Tel.: + 386 1 428 45 75
Fax: + 386 1 428 47 33
E-mail: uit@policija.si

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

Everyone has the right to request the review of relevant personal data entered in the SIS. Everyone has the right to request the correction of substantially incorrect data or the deletion of illegally obtained data entered into the SIS pertaining to him/her.

2.2. How the request should be submitted

Verbal confirmation and information given in Slovenia shall be free of charge, and any other services may only be charged according to an existing price list.

Requests can be filed in written form or also orally, for the record. Requests may also be filed at all border crossing points, administrative units and Slovenian diplomatic and consular authorities abroad. They are submitted to the Police immediately.

2.3. Minimum information to be supplied

Minimum information to be supplied: first name, last name, address, date of birth, place of birth, nationality.

2.4. Documents to be supplied

Link to the form for Request for Information on Data in the National Schengen Information System in Slovenia (N.SIS), which can be downloaded in English: https://www.iprs.si/fileadmin/user_upload/doc/obrazci/ZVOP/Zahteva%20za%20seznanitev%20s%20podatki%20v%20Schengenskem%20informacijskem%20sistemu%20v%20SI.docx

Persons who are not citizens of Slovenia must also attach a copy of a valid official document with a photo (ex. passport or ID) to this form.

2.5 Language regime

Requests may be submitted in English and Slovene language.

2.6. Link to website where information on how to apply for information/correction/deletion

3. Contact details of the national data protection authority

Informacijski pooblaščenec

(Information Commissioner)

Dunajska 22

1000 Ljubljana

Slovenia

Tel.: + 386 1 230 97 30

E-mail: gp.ip@ip-rs.si

Website: www.ip-rs.si

4. Expected outcome of requests for access. Content of the information supplied

4.1. Content of the notifications

The process of exercising the right to consult one's own personal data in Slovenia is regulated in accordance with the Act on the Protection of Personal Data in the Area of Treatment of Criminal Offences (Article 24) and the Information Commissioner Act.

Article 24 of the Act on the Protection of Personal Data in the Area of Treatment of Criminal Offences requires the Police, which is subordinate to the Ministry of the Interior and a data controller, to notify the individual whose personal data is processed about:

1. processing purposes and their legal basis;
2. types of personal data that are processed;
3. users or categories of users to whom data has been disclosed, especially if they are users in third countries or international organizations, and in cases of restrictions from the first paragraph of Article 25 of this law, only a rough description of the users may be provided;
4. the retention period of the period for regular review of the need for retention;
5. the existence of the right to request correction or deletion of data or restriction of processing and the right to file a complaint with the supervisory authority;
6. the existence of the right to file a report with the supervisory authority and its contact information;
7. all available information about the source of personal data, unless the identity of the source is protected as secret or confidential according to the provisions of the law.

The competent authority shall decide on the request without undue delay, but no later than one month after receiving the request.

The Information Commissioner is competent for deciding on an appeal by an individual whose request has been refused or the competent authority has refused to answer his application.

4.2. Procedure to submit a complaint

Applicants who consider that any of their rights have been violated in relation to the request may lodge a claim with the Information Commissioner. The Information Commissioner, having received the complaint, forwards it to the controller of the file, so that he can draw up any statements he regards as relevant. Finally, the Information Commissioner takes a decision on the complaint and forwards it to those concerned, after receiving the statements and the reports, evidence and other investigation documents, as well as inspection of the files where necessary and interviews with the person concerned and the controller of the file.

The processing of this appeal is at present free of charge.

5. References of the main national laws that apply

- The Act on the Protection of Personal Data in the Area of Treatment of Criminal Offences (Official Gazette of the Republic of Slovenia, no. 177/2020), unofficial English translation of the Act available at: <http://www.pisrs.si/Pis.web/preledPredpisa?id=ZAKO8157#>
- Information Commissioner Act (Official Gazette of the Republic of Slovenia, no. 113/2005, 51/2007 – ZUstS-A), unofficial English translation of the Act available at: <https://www.iprs.si/en/legislation/information-commissioner-act/>

3.28. SPAIN

1. Contact details of the body to which requests for access, correction or deletion should be addressed

DIVISIÓN DE COOPERACIÓN INTERNACIONAL – OFICINA SIRENE

Avda. Pío XII, 50

28016 Madrid

2. How to make an individual request and what to include in it?

The procedure is free. Any request for access must be submitted in writing together with:

- Request right of access to SIS, the format can be found in the following links:

- Application Form for the Exercise of the Right of Access SIS Document in pdf. Formulaire de Demande pour l'Exercice du Droit d' Accès au SIS pdf document.

https://www.interior.gob.es/opencms/pdf/servicios-al-ciudadano/extranjeria/acuerdo-de-schengen/sistema-de-informacion-de-schengen/sis_derecho_acceso_es_en.pdf

[División de Cooperación Internacional \(policia.es\)SIS Rights of Access Application Form \(policia.es\)](#)

[Formulario de solicitud de derecho de acceso al SIS \(policia.es\)](#)

https://www.policia.es/miscelanea/dci/formulaire_SIS.pdf

[División de Cooperación Internacional \(policia.es\)SIS Rights of Access Application Form \(policia.es\)](#)

[Formulario de solicitud de derecho de acceso al SIS \(policia.es\)](#)

- Copy of valid and valid identity document of the applicant, in which he can be fully identified.

- In case of exercising the right of access through a legal representative, in addition to the above, it will be required:

- Copy of valid and valid identity card of the representative, in which he can be fully identified.
- Document of authorisation of legal representation.

- Applications must be made through one of the following two ways:

- Submit the corresponding request addressed to:

General ADDRESS OF THE POLICY, INTERNATIONAL COOPERATION DIVISION, OFFICE SIRENE ESPAÑA,
Avda. Pio XII No. 50, 28016, MADRID

- An Electronic Registry through the SARA platform (Systems of Applications and Networks for Spanish Public Administrations and European Institutions) addressed to the address mentioned above, being necessary to be the holder of a Spanish identity document, whether it is National Identity Document, Passport or Foreigner Identity Card.

Interested parties who wish to submit a complaint related to the right of access to the Spanish Data Protection Agency can use the following link: <https://www.aepd.es/es/internacional/supervision-de-grandes-sistemas/sistema-de-informacion-schengen-sis>

2.1. Who can submit a request

- *categories of applicants that can submit a request (data subject, lawyer with power of attorney, legal guardian)*
- *representation*

Everyone has the right to exercise his or her right to know if there is information about him or her contained in the SIS, which is known as the “*exercise of the right of access*”.

2.2. How the request should be submitted

- *in person, paper and/or electronic format digitally signed (via the official electronic registry)*

- *link to online forms: <https://www.aepd.es/en/international/supervision-of-large-systems/information-system-schengen-sis>*
https://www.policia.es/misclanea/dci/formulario_sol_ejercicio_derecho_acceso_SIS.pdf
https://www.policia.es/misclanea/dci/SIS_rights_of_access_application_form.pdf
https://www.policia.es/misclanea/dci/formulaire_SIS.pdf

- *deadline to submit information: one month*

2.3. Minimum information to be supplied

- *personal data of the applicant (name, surname, date of birth, nationality, gender, citizenship);*

- use of model forms to exercise the rights vis-à-vis the SIS
- copy of the documents that proves the applicant's identity.
- in case of request for data correction or deletion, the justification for the request (e.g. corrections required, description of circumstances, reasoning for deletion)

2.4. Documents to be supplied

- proof of applicant's identity (e.g., readable copy of ID, passport, residence permit, birth certificate)

Name: Surname: Nationality: Date of birth: Identity card no. / Passport (a copy is attached): Full address:

- proof of granted power of attorney (in case of the right of access being exercised through a qualified lawyer)
- notarial verified letter of attorney or apud acta (in case of authorisation of representation by third party)

2.5 Language regime

- what language(s) can be used to submit the request: English, Spanish, French
- what language is used to reply to the applicant: Spanish.

2.6. Link to website where information on how to apply for information/correction/deletion

<https://www.aepd.es/en/international/supervision-of-large-systems/information-system-schengen-sis>
<https://www.policia.es/ es/tupolicia conocenos estructura cooperacioninternacional.php>

3. Contact details of the national data protection authority

AGENCIA ESPAÑOLA DE PROTECCION DE DATOS

Subdirección General de Inspección.

Jorge Juan 6, 28001-MADRID

Telephone +34 [900 293 183](tel:+34900293183)

Functional email address

Website <https://www.aepd.es> > es

<https://sedeagpd.gob.es/sede-electronica-web/https://sedeagpd.gob.es/sede-electronica-web/vistas/formNuevaReclamacion/identificacionSolicitante.jsf>

4. Expected outcome of requests for access. Content of the information supplied

4.1. Content of the notifications

whether personal data concerning the data subject is contained in the SIS, what is it, why and for what purpose it has been entered, by which authority.

4.2. Procedure to submit a complaint

1) confirmation of the existence of information within the system.

2) The right of access to the “Schengen Information System” is freely provided within the maximum period of one month, starting from receipt of this request,

The information shall be sent by mail to the above address within the period of ten days from the date that this request for access is granted. Furthermore, that this information shall be legible and understandable, and will include the basic data included in the Schengen Information System files from any procedure, process, or processing, as well as their source, the transferees and details of the specific uses and purposes for which they are stored.

3) the right of access can be denied in accordance with art. 24 of the national Act transposing Directive 680/2018.

5. References of the main national laws that apply

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales: <https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673>

Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales: <https://www.boe.es/buscar/act.php?id=BOE-A-2021-8806>

Those contained in art. 24 of the Spanish Organic law 7/2021 for the prevention, detection, investigation and prosecution of criminal offences or execution of criminal penalties

3.29. SWEDEN

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Polismyndigheten
Noa/IE
SE-106 75 Stockholm
SWEDEN
registrator.kansli@polisen.se

2. How to make an individual request and what to include in it?

2.2. How the request should be submitted

You are entitled to be informed whether you are registered in the SIS, unless secrecy applies. You can also make a request for deletion or correction of information which is legally or factually incorrect.

The request to be informed whether you are registered in SIS must be made in writing and signed by you, the person requesting the information. A power of attorney is not accepted (other than in exceptional cases).

2.3. Minimum information to be supplied

Please provide your name, date of birth and postal address as the Police Authority may need to send the reply by post.

2.4. Documents to be supplied

A photocopy of a valid identity document must be attached to the request, unless you indicate that the reply should be sent to your registered address in Sweden.

Forms for the request are available on the Swedish Police website:

[https://polisen.se/en/services-and-permits/police-record-extracts/schengen-information-system-sis--request-information/](https://polisen.se/en/services-and-permits/police-record-extracts/schengen-information-system-sis-request-information/)

2.5 Language regime

2.6. Link to website where information on how to apply for information/correction/deletion

3. Contact details of the national data protection authority

Integritetsskyddsmyndigheten
Box 8114
SE-104 20 Stockholm
SWEDEN

4. Expected outcome of requests for access. Content of the information supplied

4.1. Content of the notifications

4.2. Procedure to submit a complaint

Application for withdrawal of a re-entry ban

If a person has been refused entry or deported with a ban on re-entry (applicable to non-EU citizens) and wishes to apply for withdrawal of the re-entry ban, the Swedish Migration Board should be

contacted. It is the Migration Agency, or a Migration Court, which examines an application for withdrawal of a re-entry ban.

The application for withdrawal of a re-entry ban should be sent to:

Migrationsverket

SE-601 70 Norrköping

SWEDEN

Complaint to the national supervisory authority, IMY

If you want to exercise your rights, you should first turn to the Police Authority who is the authority in Sweden responsible for personal data processing in the SIS II. If you are not satisfied with how your request has been dealt with by the Police Authority, you have the right to submit a complaint to the IMY.

How to contact IMY

Phone number: +46 (0)8 657 61 00

E-mail: imy@imy.se

Website: <https://www.imy.se/en/organisations/data-protection/dataskydd-pa-eu-niva/eus-informationssystem/the-schengen-information-system/>

Integritetsskyddsmyndigheten

Box 8114

SE-104 20 Stockholm

SWEDEN

3.30. SWITZERLAND

1. Contact details of the body to which requests for access, correction or deletion should be addressed

Federal Office of Police (fedpol)
Legal department/ Data protection
Data Protection Officer
Guisanplatz 1A
CH-3003 Berne
kpr-ks@fedpol.admin.ch

2. How to make an individual request and what to include in it?

2.1. Who can submit a request

A data subject, lawyer with power of attorney or legal guardian, shall submit a request.

2.2. How the request should be submitted

Fedpol provides the opportunity to apply for information via Internet site:

- [I am submitting the application for myself \(admin.ch\)](#)
- [I am submitting the application for someone else \(admin.ch\)](#)

2.3. Minimum information to be supplied

The request shall usually be sent in writing in paper or electronic format.

Applicants do not need to justify their request for access. In case of request for data correction or deletion, the justification for the request (e.g. corrections required, description of circumstances, reasoning for deletion) has to be mentioned and the proof has to be enclosed.

The personal data (name, surname, personal address, date of birth, nationality, gender, citizenship) of the applicant has to be mentioned.

Model forms are available here:

<https://www.edoeb.admin.ch/edoeb/en/home/data-protection/dokumentation/model-letters/schengen-and-your-personal-data.html>

2.4. Documents to be supplied

The identity has to be proven by a copy of the applicant's valid passport.

2.5 Language regime

Requests can be transmitted in French, German, Italian or English.

2.6. Link to website where information on how to apply for information/correction/deletion

Further information is available [here](#).

3. Contact details of the national data protection authority

Federal Data Protection and Information Commissioner (FDPIC)
Feldeggweg 1
CH-3003 Berne
Telephone: +41(0)31 322 43 95

Fax +41(0)31 325 99 96

Contact form via website: <https://www.edoeb.admin.ch/edoeb/de/home/der-edoeb/kontakt/kontaktformular.html>

<https://www.edoeb.admin.ch/edoeb/en/home.html>

4. Expected outcome of requests for access. Content of the information supplied

4.1. Content of the notifications

Content of the notifications whether personal data concerning the data subject is contained in the SIS

4.2. Procedure to submit a complaint

In case that fedpol does not respect the individual's access request she/he can submit a complaint to the Federal Data Protection and Information Commissioner (FDPIC). The FDPIC shall open an investigation upon notification against the federal body if there are indications that a data processing operation may violate the data protection provisions. The FDPIC may refrain from opening an investigation if the breach of the data protection provisions is of minor importance. If the person concerned has filed a complaint, the Commissioner shall inform him or her of the steps taken on the basis of this complaint and the result of any investigation (Art. 22 SADP, RS 235.3 [applicable until 31.8.2023], afterwards Art. 49 of the new DSG will be applicable).

The person can also appeal to the Federal Administrative Court in accordance to Art. 48 – 53 [Administrative Procedure Act, APA](#).

5. References of the main national laws that apply

- Federal Act of 28 September 2018 on Data Protection in application of the Schengen acquis in criminal matters (SADP, RS 235.3; [DE](#); [FR](#); [IT](#))
- Federal Act of 19 June 1992 on Data Protection ([FADP; RS. 235.1](#))
- Ordinance of 14 June 1993 to the Federal Act On Data Protection (OFADP; [RS. 235.11](#))
- Ordinance on the National Part of the Schengen Information System (N-SIS) and on the SIRENE Bureau (N-SIS Ordinance; RS. 362.0; [DE](#); [FR](#); [IT](#))

ANNEX 1

MODEL LETTER FOR REQUESTING ACCESS

To: Title and address of the competent authority

Date

Dear Sir / Madam,

Pursuant to Article 53 of Regulation (EU) 2018/1861 of the European Parliament and of the Council Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and Article 67 of Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters,

I _____ (name and surname), _____ (nationality),
_____ (date and place of birth), _____ (address), would
like to request access to my personal data entered in the Schengen Information System.

Please find enclosed:

1. Copy of a valid identity document under the national law of the Schengen State (passport/identity card/driving licence (other valid identity document));
2. Copy of the legal authorisation to represent the applicant;
3. Other.

The Applicant / The Legal Representative

(SIGNATURE)

ANNEX 2

MODEL LETTER FOR REQUESTING RECTIFICATION

To: Title and address of the competent authority

Date

Dear Sir / Madam,

Pursuant to Article 53 of Regulation (EU) 2018/1861 of the European Parliament and of the Council Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and Article 67 of Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters,

I _____ (name, surname), _____ (nationality),
_____ (date and place of birth), _____ (address),
would like to request rectification of factually inaccurate data relating to me stored in the Schengen Information System. My personal data should be rectified because:

Please find enclosed:

1. Copy of a valid identity document under the national law of the Schengen State (passport/identity card/driving licence (other valid identity document));
2. Copy of the legal authorisation to represent the applicant;
3. Other elements justifying the need for rectification.

The Applicant/ The Legal Representative

(Signature)

ANNEX 3

MODEL LETTER FOR REQUESTING ERASURE

To: Title and address of the competent authority

Date

Dear Sir / Madam,

Pursuant to Article 53 of Regulation (EU) 2018/1861 of the European Parliament and of the Council Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and Article 67 of Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters,

I _____ (name and surname), _____ (nationality),
_____ (date and place of birth), _____ (address), would like to request rectification of factually inaccurate data relating to me or deletion of data relating to me which have been unlawfully stored in the Schengen Information System. My personal data should be erased because:

Please find enclosed:

1. Copy of a valid identity document under the national law of the Schengen State (passport/identity card/driving licence (other valid identity document);
2. Copy of the legal authorisation to represent the applicant;
3. Other elements justifying the need for erasure.

The Applicant/ The Legal Representative

(Signature)

2020-2022

Adopted on 6 July 2022

Coordinated Supervision Committee Report of Activities



Table of contents

1. FOREWORD	3
2. ABOUT THE COORDINATED SUPERVISION COMMITTEE	5
2.1 Mission	6
2.2 Tasks & duties	6
3. 2020-2022: AN OVERVIEW	7
3.1 Setting up the CSC	7
3.1.1 <i>Rules of Procedure</i>	7
3.1.2 <i>Organisation of meetings</i>	7
3.1.3 <i>Working methods</i>	8
4. ACTIVITIES	
4.1 Promote and facilitate the exercise of data subject rights	9
4.1.1 <i>Report on the use of the IMI system with proposals on the exercise of data subject rights</i>	9
4.1.2 <i>List of national competent supervisory authorities</i>	10
4.2 Examine difficulties of interpretation or application of EU and national law	10
4.2.1 <i>Discussions about the interplay between EU and national law and its application to the activities of supervisors</i>	10
4.3 Exchange information and conduct joint audits or coordinated inspections	11
4.4 Prepare for the start of the EPPO's activities and other EU bodies and information systems that will fall under the Committee's scope	11
4.4.1 <i>EPPO</i>	11
4.4.2 <i>Europol</i>	11
4.4.3 <i>Preparation of the new large-scale EU Information Systems</i>	11
5. MAIN OBJECTIVES FOR 2022-2024	13
5.1 Getting ready for the new large-scale EU Information Systems	13
5.2 Coordination and effective supervision	14
5.2.1 <i>Promote and facilitate the exercise of data subject rights</i>	14
5.2.2 <i>Examine difficulties of interpretation or application of EU and national law</i>	14
5.2.3 <i>Exchange information and conduct joint audits or coordinated inspections</i>	14



1. FOREWORD

Over the last years, EU large-scale information systems connecting EU Member States' authorities and EU bodies (EUIs) have increased and evolved. Through these systems, the EUIs and national authorities share personal data electronically, with an unprecedented speed and volume. For instance, in 2019 alone, 58,396 information exchanges were sent through the Internal Market Information System (IMI)¹ on very diverse policy areas such as firearms authorisations, GDPR, e-commerce, services and patients' rights. In the law enforcement field, during 2020, the EU Agency for Criminal Justice Cooperation (Eurojust)² registered in its information system 4700 new cases, while provided assistance to 8800 cross-border criminal investigations. It supported 268 Joint Investigation Teams, facilitated the execution of 1284 European Arrest Warrants, enabled the use of 1359 European Investigation Orders and extended the network of Eurojust contact points to 55 countries.

To make sure that these processing operations are in line with the EU's data protection framework, supervision is two-fold: the European Data Protection Supervisor (EDPS) supervises the EU bodies' processing of personal data, while national data protection Supervisory Authorities (SAs) supervise data processing by the national competent authorities (e.g. administrative, police, border authorities,

judiciary). It is thus essential that the EDPS and national SAs coordinate their supervisory activities.

With the entry into application of [Regulation 2018/1725](#) in December 2019, this cooperation between the EDPS and the national Supervisory Authorities came within the framework of the European Data Protection Board. To steer this cooperation and the monitoring activities in the right direction, the Coordinated Supervision Committee (CSC) was established. The Committee aims to enhance cooperation among the different Supervisory Authorities and ensure a more effective supervision. It co-ordinates the supervision of those EU large-scale information systems and bodies whose legal acts refer to Article 62 of Regulation 2018/1725 or to the European Data Protection Board, and by implication, to the CSC.

Over the last two years, the Internal Market Information System (IMI), Eurojust, the European Public Prosecutor's Office (EPPO) and Europol have come into the scope of the CSC. Gradually, the Committee will also cover other IT systems, bodies, offices and agencies in the fields of Border, Asylum and Migration (SIS, EES, ETIAS and VIS), Police and Justice Cooperation (SIS, ECRIS-TCN) and the next generation Prüm.

1. https://ec.europa.eu/internal_market/imi-net/statistics/2021/02/exchanges/index_en.htm

2. [Eurojust Consolidated Annual Activity Report 2020](#)

This bi-annual report summarises the work completed by the CSC during the first two years of its existence. While a large part of the CSC is still under construction, the Committee has been working full speed to accommodate the large-scale information systems that have already come under its purview and to prepare the arrival of the others. Since December 2019, it has been closely following developments at IMI and Eurojust, as well as EPPO from June 2021 onwards, and Europol from June 2022. In December 2021, the first report was published concerning the use of the Internal Market System in the EU Member States.

Looking forward to the coming years, the CSC is ready to welcome more IT systems & EUIs within its purview. It will tackle the outstanding items in the work programme and continue to assist SAs in their work, by providing further clarification on the interpretation of EU and national law, stimulating the exchange of information and best practices, and providing support for joint audits or coordinated inspections.

Clara Guerra
CSC Coordinator





2. ABOUT THE COORDINATED SUPERVISION COMMITTEE

In accordance with Article 62 of Regulation 2018/1725, the national Supervisory Authorities (SAs) and the European Data Protection Supervisor (EDPS) shall cooperate actively to ensure effective supervision of large-scale IT systems and of EU bodies, offices and agencies. For this purpose, they shall meet at least twice per year within the framework of the EDPB. Additionally, several legal acts on large-scale IT systems and EU agencies refer to this model of coordinated supervision.

To ensure the consistency of supervision efforts on both levels, all SAs involved, including the EDPS, used to cooperate through Supervision Coordination Groups (SCGs). Each of these groups was dedicated to a specific EU database. Since December 2018, Regulation 2018/1725 has provided for a single model of coordinated supervision for large-scale EU IT systems and agencies within the framework of the EDPB. This replaces the current system of individual SCGs. The new model does not apply to all EU information systems and agencies at once, but progressively, according to when the revised version of the establishing act of each EU information system and agency becomes applicable.

In December 2019, the Coordinated Supervision Committee (CSC) was formally established within the EDPB. It brings together the SAs of each EU Member State and the EDPS, as well as SAs of non-EU Members of the Schengen Area when foreseen under EU law. During its first meeting, Giuseppe Busia from the Italian SA was elected as Coor-

dinator and Iris Gnedler from the German federal SA as Deputy Coordinator for a term of two years.

In December 2020, the CSC elected Clara Guerra from the Portuguese SA to succeed Giuseppe Busia as the CSC Coordinator, due to Mr. Busia's departure from the Italian SA and thus from the CSC. Sebastian Hümmeler from the German Federal SA was elected in December 2021 to succeed Ms. Gnedler as Deputy Coordinator, upon the end of her two years term.

Participation in the CSC meetings can occur under various arrangements, depending on the IT system, body, office or agency for which supervision is taking place, as well as the respective EU legal act.

Likewise, cooperation within the CSC can take many forms, ranging from exchanging information and assisting each other in carrying out audits and inspections to preparing harmonised proposals for solutions to identified problems and promoting awareness of data protection rights.

While the Committee is established within the framework of the EDPB, it enjoys an autonomous functioning and positioning, pursuant to Article 37.2 of the [EDPB Rules of Procedure](#). The Committee adopts its own rules of procedure and working methods. The EDPB Secretariat provides the Secretariat of the CSC.

2.1 Mission

The CSC ensures the coordinated supervision by Supervisory Authorities of large-scale IT systems and of EU bodies, offices and agencies falling under its scope, in accordance with Article 62 of Regulation (EU) 2018/1725 or with the EU legal act establishing the large-scale IT system or the EU body, office or agency.

The following EU large-scale IT systems, bodies, offices and agencies currently fall under the CSC's scope:

Internal Market:

- [Internal Market Information System \(IMI\)](#), which allows the exchange of information between public authorities involved in the practical implementation of EU law.
 - The CSC ensures coordination in the supervision of the processing of personal data in the Internal Market Information System (IMI) in accordance with Article 21 of Regulation (EU) No 1024/2012 (as modified by Article 38 of Regulation (EU) No 2018/1724).

Police and Judicial Cooperation:

- [Eurojust](#), the agency responsible for judicial cooperation in criminal matters among EU Member States.
 - The CSC ensures coordination in the supervision of the processing of operational personal data in the context of cooperation between the national members within Eurojust in accordance with Article 42 (2) of Regulation (EU) No. 1727/2018.
- [European Public Prosecutor's Office \(EPPO\)](#), the prosecution agency responsible for investigating, prosecuting and bringing to judgment crimes against the EU budget.
 - The CSC ensures the coordination in the supervision of the processing of operational personal data with respect to specific issues requiring national involvement, in particular, if there are major discrepancies between practices of EU Member States, potential unlawful transfers using the EPPO communication channels, or questions raised by one or more national SAs on the implementation and interpretation of Regulation (EU) No. 1939/2017, in accordance with its Article 87.

- [Europol](#), the agency responsible for police cooperation among EU Member States.

→ The CSC ensures the coordination in the supervision of the processing of operational personal data in the context of the support by Europol to the national competent authorities of the Member States and their mutual cooperation in combatting serious crime, since the recent entry into force on 28 June 2022 of the recast of the Europol Regulation (EU) 2016/794, in accordance with Article 44 (2), amended by Regulation (EU) No. 2022/91.

2.2 Tasks & duties

Within its mission to ensure the coordinated supervision of some large-scale IT systems and of EU bodies, offices and agencies, the CSC can:

- Exchange relevant information;
- Assist the Supervisory Authorities in carrying out audits and inspections;
- Examine difficulties of interpretation or application of the EU legal act establishing the large-scale IT system or the EU office, body or agency subject to coordinated supervision;
- Study problems with the exercise of independent supervision or with the exercise of the rights of data subjects;
- Draw up harmonised proposals for solutions to problems;
- Promote awareness of data protection rights.



3. 2020-2022: AN OVERVIEW

3.1 Setting up the CSC

3.1.1 Rules of Procedure

The [Rules of Procedure](#) were adopted during the first meeting of the Coordinated Supervision Committee, which took place on 3 December 2019. They outline the most important procedural rules of the CSC. They describe:

- The CSC's guiding principles;
- The CSC's composition;
- The CSC's organisation;
- The election of its coordinator and deputy coordinators;
- The CSC's working methods.

3.1.2 Organisation of meetings

The Committee must meet at least twice a year. The Coordinator may also decide to convene extraordinary meetings, on his/her own initiative or at the request of the majority of the Committee's participating authorities.

The COVID-19 crisis has led EU institutions to adapt to new ways of working and to hold meetings remotely to be able to

continue their activities. The Committee has also resorted to remote meetings and will need to do so again in the future.

Participation in the CSC meetings can occur under various arrangements, depending on the IT system, body, office or agency for which supervision is taking place, as well as the respective EU legal act:

- IMI: The EDPS and the national Supervisory Authorities (SAs) of the 27 EU Member States participate in the activities of the CSC in relation to IMI. The national SAs of Iceland, Liechtenstein, and Norway also participate, as their respective countries also apply the EU legal acts governing IMI;
- Eurojust: The EDPS and the national SAs of 26 EU Member States participate in the activities of the CSC in relation to Eurojust;
- EPPO: The EDPS and the national SAs of the 22 participating EU Member States participate in the activities of the CSC in relation to the EPPO;
- Europol: The EDPS and the national SAs of 26 EU Member States participate in the activities of the CSC in relation to Europol.

An overview of the CSC members and their participation in relation to the respective IT system, body, office or agency can be found on the [CSC webpage](#).

3.1.3 Working methods

The Committee elects a Coordinator and at least one Deputy Coordinator from among its members for a term of office of two years.

The Coordinator convenes and chairs the meetings, acts as a contact point in CSC matters, sets the draft agenda, carries out all the tasks that have been assigned to them in the Rules of Procedure and updates the European Data Protection Board of the work of the Committee at least twice a year. The Deputy Coordinator will perform these tasks if the Coordinator is unable to attend. Both cooperate in liaison with the EDPB Secretariat to ensure the smooth functioning of the Committee, prepare the draft agenda, the draft work programme, and the draft joint report of activities on coordinated supervision.

The Secretariat of the Committee is provided by the EDPB Secretariat. The Secretariat assists the Committee in the performance of its tasks and acts solely in the best interests of the Committee.

The Committee or the Coordinator may designate one or several (co-) rapporteur(s) for specific issues. The rapporteurs are responsible for the elaboration of documents, incorporating comments into revised drafts, finalising the documents, and presenting them to the Committee.

The Committee created its own logo and a dedicated website, within the EDPB's website, to communicate on its work with the public. On this website, the Committee publishes general information, documents it produces, and summaries of its meetings' discussions, in accordance with Article 9 of the [CSC Rules of Procedure](#).

As mentioned in its [Work Programme 2020-2022](#), the Committee seeks through its activities and meetings a regular dialogue and engagement with controllers, processors and third parties, including civil society organisations, to ensure a comprehensive reflection on the issues at stake, while always taking into account its role as an independent body.





4. ACTIVITIES

In line with its biannual work programme, the Committee carried out the following main activities from 2020 to 2022:

1. Promote and facilitate the exercise of data subject rights;
2. Examine difficulties of interpretation or application of EU and national law;
3. Exchange information and conduct joint audits or coordinated inspections;
4. Prepare for the start of the EPPO's activities and other EU bodies and information systems that will fall under the Committee's scope.

4.1 Promote and facilitate the exercise of data subject rights

One of the main legal tasks of the Committee is to study problems related to the exercise of independent supervision or the exercise of data subject rights and to propose solutions to these problems.

Large-scale EU information systems and networks such as IMI, Eurojust, and EPPO, which connect EU and national authorities seamlessly, have a hybrid nature: both national-EU and trans-European. Data may transit and be stored in multiple places and be processed by diverse entities. Data subjects may not know at a given point in time if their data is being processed at EU and/or at national level. As such, they may not know to whom they can address their requests.

The Committee focused its activity on the exercise of data subjects rights in relation to IMI, by identifying the current practices, based on an evaluation of the level of compliance at national level, carried out in a coordinated manner, in order to decide on the joint action to be taken to tackle the deficiencies found.

4.1.1 Report on the use of the IMI system with proposals on the exercise of data subject rights

The Committee requested and received information on the retention of personal data in the IMI system and the users with access to it, the information recorded in the IMI logs and the information available to data subjects from the European Commission. The European Commission confirmed that there are no common European templates with information for data subjects on how they may

exercise their rights at national level in relation to the processing in IMI of their personal data.

The Committee subsequently discussed how to ensure that data subjects have access to sufficient information on the exercise of their rights with respect to the processing of their personal data in IMI.

Before taking concrete and coordinated actions, the CSC members decided to obtain more information on the use of IMI and, in particular, on the information available to data subjects on IMI at national level.

To this end, the Committee prepared a questionnaire, to be filled out by its members in consultation with the national IMI Coordinators (NIMIC), on the use of the Internal Market Information System (IMI) in their respective countries by various authorities (including data protection authorities) to process personal data.

The questionnaire consisted of four parts: questions about the general implementation of IMI in the Member State, questions about data subject rights, questions about the information policy in the Member State, and questions about the implementation of IMI in the supervisory authority.

In December 2021, the Committee produced a [report](#) based on the responses to the questionnaire obtained from the CSC members. The report provides a general overview of the use of IMI and will form the basis for the CSC's future work on this topic.

The report identifies some diversity among the EU Member States in their use of IMI concerning the number of registered authorities and users, the practice of access allocation, and the roles in place in the system. In other areas, there were fewer discrepancies, for example concerning the tasks performed by the National IMI Coordinators (NIMIC) and the general rules for assigning user rights.

The responses further showed that in the majority of Member States, data subjects' requests are dealt with directly by the controllers (i.e. the competent authorities) and there is therefore no centralised view in terms of the number of requests received.

In terms of the information policy at national level for IMI, a significant number of the Committee members indicated that they considered either that controllers do not provide sufficient information about IMI, or they were not in a position to respond to this.

In view of the conclusions taken, the CSC decided that it would develop recommendations to the national competent authorities, as controllers, regarding GDPR transparency obligations for the IMI data processing. These recommendations should include a standardised text model to be used on a voluntary basis by the controllers.

4.1.2 List of national competent supervisory authorities

After discussing the information available to data subjects on the exercise of their rights in relation to the processing of their personal data in the IMI at the EU and national level, the Committee drew up an [updated list of national Supervisory Authorities competent to receive complaints or any other referrals from data subjects](#) concerning IMI, Eurojust and EPPO with their contact details and made it available to the public via the Committee's public website.

4.2 Examine difficulties of interpretation or application of EU and national law

Another legal task of the Committee is to examine difficulties of interpretation or application of Regulation 2018/1725 and other EU laws to their activities in relation to EU large-scale information systems and bodies.

In order to effectively, and in harmonized manner, apply EU law to their activities, Supervisory Authorities need to reach a common understanding on the interplay between EU instruments with a general nature (such as Regulations 2018/1725 and Directive 2016/680) and those with a specialised nature (such as the IMI, Eurojust and EPPO Regulations).

The application of some of these EU instruments also needs to be reconciled with the application of national law, which may apply for instance to the processing of law enforcement data.

4.2.1 Discussions about the interplay between EU and national law and its application to the activities of supervisors

The Committee members took note of and considered the study commissioned by the EDPB on data protection in the judiciary and the concept found in the GDPR and in the EU Data Protection Law Enforcement Directive (LED)³ of courts/judicial authorities acting in their judicial capacities.

³. [Directive \(EU\) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.](#)

The Committee received a presentation from the Eurojust DPO on Eurojust's functioning, its legal basis, its processing of personal data and the attribution of responsibilities. The Committee discussed the interpretation and application of Article 42 of the Eurojust Regulation - "Cooperation between the EDPS and national Supervisory Authorities"- and a proposal for cooperation between Supervisory Authorities and law enforcement authorities in the area of cybercrime.

The Committee also discussed its preparation for the entry into operation of the European Public Prosecutor's Office (EPPO) on 1 June 2021. The Committee members received presentations from an academic, who had studied the interpretation of the EPPO Regulation in view of its supervision by the EDPS and the self-monitoring by the EPPO DPO. The discussions addressed the interplay between the regulations applicable to the EPPO's processing of data, as well as controllership over the personal data in question. The Committee also discussed the next steps to be taken regarding the supervision of the EPPO at the European and national level.

4.3 Exchange information and conduct joint audits or coordinated inspections

Another of the Committee's key tasks is to enable Supervisory Authorities to exchange relevant information and assist each other in carrying out audits and inspections. Information exchange and mutual assistance are necessary because of the complexity and size of the information systems supervised, the transition and retention of personal data across various national and EU information systems, and the multiple and diverse data controllers, processors, data subjects and other parties that may be involved.

Supervisory Authorities are already experienced in supervising EU bodies and large-scale information systems such as Europol, SIS, CIS, Eurodac and others. Building on this experience, they sought to identify those processing operations or practices involving personal data in relation to IMI, Eurojust and the EPPO that require or could benefit from an exchange of information and assistance at European level.

In this context, the Committee members discussed how to prepare a common European-wide framework for audits of IMI conducted at the national level.

The Committee also engaged with Eurojust representatives, including its DPO, to obtain more information on matters such as the Eurojust Counter-Terrorism Register, the communication channels used between national authorities and Eurojust to exchange information, and other data protection matters. In addition, the EDPS presented the draft report on its audit on Eurojust, which took place

on 25-26 October 2021. The audit was based on consultation with the agency. Its scope focussed on the processing of operational data only and on areas subject to legislative changes. The Committee took note of the EDPS' audit and identified issues for follow-up at national level.

4.4 Prepare for the start of the EPPO's activities and other EU bodies and information systems that will fall under the Committee's scope

4.4.1 EPPO

The European Public Prosecutor's Office (EPPO) started its operations in June 2021. The Committee has closely followed the EPPO's implementation at Member State level.

After having obtained information from the EPPO DPO, the Committee decided that its members should engage with the European Delegated Prosecutors (EDPs) in their respective Member States. The objective was to open communication channels with them, to obtain more information on the state of play of the EPPO's start of operations at national level and to learn about their interaction with the national competent authorities (such as courts and law enforcement authorities) and the use of relevant national systems and databases. To this end, the Committee prepared a common questionnaire and discussed the answers provided by its members.

The Committee discussed the national legal framework and the organisation of the EDPs' work environment, in particular the communication with EPPO and the interaction with other national competent authorities. The Committee noted that in many Member States the EDPs are still being set up and that there were some delays and provisional arrangements. The Committee will continue to monitor closely the EPPO's implementation and the need for advice during this phase.

4.4.2 Europol

The Committee began preparing for its role in the coordinated supervision of Europol, which fell under the Committee's purview on 28 June 2022. The Committee engaged with the Europol Cooperation Board (ECB) and its Secretariat to prepare this transition.

4.4.3 Preparation of the new large-scale EU Information Systems

The Committee noted that eight additional EU information systems are expected to fall under its purview in the

coming two years. These systems are of a technical and complex nature and raise especially sensitive data protection issues. Some of these issues will result from the foreseen interoperability between them.

In the future, the CSC will become the single forum for data protection coordinated supervision of the EU systems. This horizontal approach will enable DPAs to have a holistic view of all the data processing involved, including the multiple cross-access rights from EU agencies to different systems, as well as the envisaged interoperability among several EU information systems, and to be more effective in their monitoring activities.

In light of the above and to prepare its coordinated supervision over these information systems, the Committee discussed its future internal organisation and working methods. The CSC members underlined the need for the CSC to be flexible in this regard.

While complying with the requirement to hold at least two meetings per year, the CSC will hold an increased number of meetings, whose attendance will vary in accordance with the systems being discussed. The meetings will be organised, preferably, based on three configurations (border management, police and judicial cooperation, IMI). It will still be possible to have combined configurations, if necessary, for general affairs, specific items or coordinated actions.

The Committee addressed additional matters, such as access to the information of the supervision coordinated groups, from which it will take over coordinated supervision, the need for a secure platform for the handling of documents, and cooperation with external stakeholders, in particular those from other EU bodies, such as the EU Agency for Fundamental Rights (FRA), Joint Research Centre (JRC), European Union Agency for Law Enforcement Training (CEPOL) or European Union Agency for Cybersecurity (ENISA), and NGOs working in relevant areas.

The Committee also began preparing for the entry into operation of new information systems by inviting technical experts to discuss their future operations and identify high risks in relation to data protection.

In this context, the Committee received a presentation from a representative from FRA on its last research on EU large-scale IT systems and their interoperability, with a focus on the Entry Exit System (EES), the European Travel Information and Authorisation System (ETIAS), and the EU Interoperability Regulations.

The Committee also identified some of the files it could soon inherit from the Europol Cooperation Board (ECB) and the SIS II Supervision Coordinated Group (SIS II SCG).



5. MAIN OBJECTIVES FOR 2022-2024

Two years after the creation of the CSC, the Committee is looking ahead and evaluating where its focus should be in the coming years. A high number of additional EU agencies and information systems will fall under the CSC's purview in 2022 and 2023. The Committee will continue adjusting its working methods and organisation of meetings to cover them effectively. The Committee will engage with existing coordinated supervision groups on specific EU information systems and agencies and with the EDPS, which provides the secretariat for these SCGs, to prepare their transition to the CSC.

For the next biennium, the Committee will focus on providing clear guidance to data subjects about their data protection rights vis-à-vis the several EU information systems and how they can in practice exercise them.

The Committee will strive to reach a holistic view considering the interaction and interoperability of the European information systems, in order to improve effectiveness in the coordinated supervision activities.

5.1 Getting ready for the new large-scale EU Information Systems

The Committee will continue its preparations to assume the coordinated supervision over the EU information systems and agencies that will fall within the scope of the CSC.

The following IT systems, bodies, offices, and agencies will gradually be moved to the CSC:

Border, Asylum and Migration:

- Schengen Information System (SIS), which ensures border control cooperation (before the end of 2022);
- Entry Exit System (EES), which registers entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Schengen States (expected in 2023);
- European Travel Information and Authorisation System (ETIAS), which tracks visitors from countries who do not need a visa to enter the Schengen Zone (expected in 2023);
- Visa Information System (VIS), connecting consulates in non-EU countries and all external border-crossing points of Schengen States (expected in 2023);
- Eurodac, which compares fingerprints of asylum applicants to see if they have previously applied for asylum or entered the EU irregularly via another Member State (expected in 2023);

- Customs Information System (CIS), which is an automated information system that assists EU State administrative authorities in preventing, investigating and prosecuting operations that are in breach of customs or agricultural legislation (No estimated date for the entry into force and the date of application of legislative proposal).

Police and Judicial Cooperation:

- SIS, which also ensures law enforcement cooperation (before the end of 2022);
- European Criminal Records Information System on third country nationals (ECRIS-TCN), which allows EU Member State authorities to identify which other Member States hold criminal records on third country nationals or stateless persons being checked (expected in 2023);
- In addition, the interoperability of EES, Eurodac, ETIAS, ECRIS-TCN, SIS, and VIS is expected to go live by the end of 2023.

5.2 Coordination and effective supervision

5.2.1 Promote and facilitate the exercise of data subject rights

The CSC will continue its work to facilitate the exercise of data subject rights vis-à-vis the large-scale information systems within its purview. Among others, the CSC will develop recommendations to the national competent

authorities, as controllers, regarding GDPR transparency obligations for IMI data processing. In addition, the CSC will work on guidance regarding the different EU information systems and continue to exchange best practices.

5.2.2 Examine difficulties of interpretation or application of EU and national law

The CSC will continue its work in this area to ensure the effective application of EU law by Supervisory Authorities and to clarify the interplay between national and EU law where relevant.

5.2.3 Exchange information and conduct joint audits or coordinated inspections

As one of the Committee's main raisons d'être, the CSC will continue to promote the exchange of information among its members and to provide support for joint audits or coordinated inspections. Among others, the CSC plans to develop general standards or reference frameworks for national audits and inspections. In addition, the Committee will work to promote best practices based on the Committee members' experience supervising EU large-scale information systems and bodies

The Committee will explore avenues for an effective dialogue between Supervisory Authorities and public authorities acting as data controllers, such as the European Commission, Eurojust, Europol and the EPPO, which could be beneficial for them and in turn, for EU citizens. Such dialogue should also involve civil society organisation to ensure a comprehensive reflection on the issues at stake.

CONTACT DETAILS

Postal adress
Rue Wiertz 60, B-1047 Brussels

Office adress
Rue Montoyer 30, B-1000 Brussels



Coordinated
Supervision
Committee



Work Programme 2022-2024

Adopted on 6 July 2022

Work Programme 2022-2024

Contents

1. INTRODUCTION	3
2. WORKING METHODS	4
2.1 Distribution of roles	4
2.2 Organisation of the meetings	4
2.3 Technical tools	5
2.4 Communication with the public.....	5
2.5 Dialogue and engagement with stakeholders	5
3. PLANNED ACTIVITIES.....	6
3.1 Promote and facilitate the exercise of data subject's rights	6
3.2 Examine difficulties of interpretation or application of EU and national law	7
3.3 Exchange information and conduct joint audits or coordinated inspections.....	7
3.4 Prepare the coordinated supervision of EU bodies and information systems that will fall under the Committee's scope	9

1. INTRODUCTION

The Coordinated Supervision Committee (CSC) hereby presents its second work programme for the biennium 2022-2024 directly after Europol came under its purview. This most recent addition to the tasks of the CSC entails the coordination between the national data protection supervisory authorities (SAs) and the European Data Protection Supervisor (EDPS) in the supervisory activities of the biggest EU information hub for police cooperation.

Within the context of the CSC, Europol joins the EU Agency for Criminal Justice Cooperation (Eurojust) and the European Public Prosecutor's Office (EPPO), forming a trilogy of information systems in a field where processing of personal data has a huge impact on the rights of individuals. This is even more evident with the increased technical capacity of accessing data from multiple sources, public and private, of crosschecking and further processing large sets of data, and of using AI tools to carry out analysis and seek patterns.

This reality requires constant and effective monitoring from data protection authorities to ensure that the level of interference with the fundamental rights to data protection and privacy as provided for by the EU Charter is really necessary and proportionate to accomplish the important public interest of combatting serious and organised crime, including terrorism.

Building also on the experience of the precedent bodies of the CSC such as the Europol Cooperation Board, the CSC will intensify its supervisory activities in all systems within its remit, through coordinated targeted actions, based on enhanced cooperation and information exchange between the EDPS and the national SAs to ensure effective results.

In the next two years, new EU systems will be set up. Within the same period, existing EU systems will be renewed with extended functions, such as the Schengen Information System (SIS). Characteristic to these developments is the focus on interoperability between systems. The CSC therefore already includes a coordinated supervisory activity covering both Europol and SIS in the current work programme. This initiative takes advantage of the horizontal approach in supervision that favours a holistic view of all the data processing involved and of all the interactions among systems.

This work programme has selected the data subjects' rights as a key-area of activity. The CSC will reinforce awareness raising and it will provide more guidance to assist individuals in navigating the network of systems and controllers and the great number of different rules when exercising their rights, also in view of the challenges the interoperability legal framework will bring.

The CSC is also committed to improve its dialogue with stakeholders, in particular with NGOs, academia and researchers working in this field, by promoting reflection and debate on issues of common interest. Transparency is a guiding principle to our work and the CSC will use its website in a more intense way, within the European Data Protection Board (EDPB), to communicate with the public and to report on its activities.

This is undoubtedly an ambitious work programme. Not only are we still in a transitional phase of implementation of systems while recasting the legal framework, but mostly due to the insufficient financial and human resources allocated to the majority of the data protection supervisory authorities. Yet it is imperative that we are able to perform our legal tasks at national and at EU level. The CSC is

firmly committed to do so to ensure that all individuals can enjoy of an effective EU area of freedom, security and justice.

2. WORKING METHODS

2.1 Distribution of roles

The Committee elects a Coordinator and at least a Deputy Coordinator from among its members for a term of office of two years.¹

The Coordinator convenes and chairs the meetings, acts as a contact point in CSC matters, sets the draft agenda, carries out all the tasks that have been assigned to him/her in the Rules of Procedure and updates the European Data Protection Board of the work of the Committee at least twice a year. The Deputy Coordinator will perform these tasks if the Coordinator is unable to attend. Both cooperate in liaison with the Secretariat to ensure the smooth functioning of the Committee, prepare the draft agenda, the draft work programme and the draft joint report of activities on coordinated supervision the Committee will adopt.²

The EDPB Secretariat will also provide the Secretariat of the Committee.³ The Secretariat assists the Committee in the performance of its tasks and acts solely in the best interests of the Committee.

The Committee or the Coordinator may designate one or several (co-) rapporteur(s) for specific issues. They will be responsible for the elaboration of documents, incorporating comments into revised drafts, finalizing the document and presenting them to the Committee.⁴

2.2 Organisation of the meetings

The Committee must meet at least twice a year.⁵ The Coordinator may also decide to convene extraordinary meetings, on its own initiative or at the request of the majority of the Committee's participating authorities.⁶ The Secretariat shares the invitations, the draft agenda and the meeting documents with each member of the Committee at least 10 days in advance of the meeting.⁷ In exceptional circumstances, documents may be distributed later.

Meetings of the Committee can only take place if at least half of the participating authorities or their representatives are attending.⁸ The Committee will approve the agenda at the beginning of each meeting.⁹

The costs and the servicing of the Committee's meetings are borne by the EDPB Secretariat.

¹ Article 3 of the Rules of Procedure

² Article 4 of the Rules of Procedure

³ Article 17 of the Rules of Procedure

⁴ Article 8 of the Rules of Procedure

⁵ Article 12.1 of the Rules of Procedure

⁶ Article 12.3 of the Rules of Procedure

⁷ Article 14 of the Rules of Procedure

⁸ Article 12.5 of the Rules of Procedure

⁹ Article 13.4 of the Rules of Procedure

The COVID-19 crisis has led EU institutions to adapt to new ways of working and to hold meetings remotely to be able to continue their activity. The Committee has also resorted to remote meetings to hold its meeting of 8 July 2020. The pandemic has also stimulated the creative spirit of its members, and a new form of meeting has been introduced since April 2022: hybrid meetings.

In ordinary times, remote meetings can also be a useful way to lighten the agenda of the Committee in-person meetings, improve the Committee's efficiency and the quality of its work. The Committee could organize remote meetings to address matters that could be discussed briefly and/or that could not wait for the in-person meetings. The Committee could leave to in-person meetings matters that may be more complex and require longer discussions.

More generally, the Committee discussed its internal functioning. The Committee also noted the high number of additional EU agencies and information systems that will fall under the CSC's purview this year and in 2023 and launched its reflection on how to organise its working methods and meetings to cover them effectively.

The Committee discussed and agreed with the proposals presented for the future functioning of the CSC. The Committee will strive to reach a holistic view considering the interaction and interoperability of the European information systems, in order to improve effectiveness in the coordinated supervision activities. The Committee also opted for flexible working methods and will enhance cooperation with external stakeholders.

2.3 Technical tools

The Committee has a functional mailbox within the EDPB mailbox for all correspondence of the Committee. The Secretariat is in charge of handling this functional mailbox, answering questions and requests of members and redirecting emails from third parties to the Coordinator or participating authorities where needed. The Secretariat also uses the functional mailbox to issue the invitations, the draft agenda and the documents for the meetings.

The Secretariat also uses the Confluence system as its main tool for sharing information with the participants. The Committee has a dedicated section with a forum, subsections for each of the CSC meetings, a section for the work items overview, and resources made available and/or produced by the CSC members, such as legal references, interpretative guidelines, best practices and others.

2.4 Communication with the public

The Committee has a dedicated website where all public documents of the Committee are available. The webpages will be updated with the new relevant information on the EU information systems whose coordinated supervision comes under the CSC.

2.5 Dialogue and engagement with stakeholders

The Committee should seek, through its activities and meetings, a regular dialogue and engagement with controllers, processors and third parties, including civil society organisations to ensure a

comprehensive reflexion on the issues at stake, while always taking into account its role as independent body.

3. PLANNED ACTIVITIES

The Committee has planned the following activities in the work programme to:

- Ensure that data subjects are able to exercise their rights;
- Promote the exchange of information and joint audits or coordinated inspections by national SAs and the EDPS;
- Reach a common understanding between its participating authorities on their respective scope of supervision, applicable legal basis, and the areas where they need to cooperate and coordinate;
- Prepare the Committee's work on the supervision of the EU bodies and information systems that will fall within the Committee's remit in the coming years.

The Committee will be flexible and work on other activities that may not be included in this work programme but that participating authorities may bring to its attention, based on their relevance, urgency or unforeseen character.

3.1 Promote and facilitate the exercise of data subject's rights

The Committee will carry out the following tasks under this activity:

- **Make recommendations to controllers on the exercise of their data protection obligations, such as on the information provided to data subjects:**
 - Draft IMI guidance on transparency.
- **Elaborate guidance on the rights of data subjects regarding the different EU information systems and how the data subjects can exercise them, including information on competent authorities for handling the requests:**
 - Draft new guides of access for EPPO, Eurojust and the new set-up systems.
 - Update existing guides of access for SIS and Europol in view of the new legal frameworks.
 - Work on the consolidation in one-single document of the exercise of rights vis-à-vis the different information systems, as a roadmap for data subjects to navigate among systems, controllers, formalities for submission, deadlines for replies, and so forth, having the possibility to have updates in order to integrate new systems as they come along.
 - Monitor the implementation of the web portal for data subjects exercising their rights, as provided for in Article 49 of the interoperability regulations, also in view of the delegated act to be adopted by the Commission in this regard.

- Coordinate on the national implementation of the Schengen information campaigns and cooperate with the European Commission pursuant Article 19 of Regulation (EU) 2018/1861 and Article 19 of Regulation (EU) 2018/1862.
- Monitor the impact on the rights of individuals by the implementation of recent developments in the legal framework, in particular in relation to interoperability and the role of Europol.
- Draft a report from information provided by national competent authorities in Member States to the EDPB¹⁰ on the exercise of the data subjects' rights, on court proceedings and on mutual recognition of final decisions to be included in the joint report of activities regarding the Schengen Information System.
- Exchange best practices on data subject's rights.

3.2 Examine difficulties of interpretation or application of EU and national law

The Committee will carry out the following tasks under this activity:

- Continue studying the interplay between EU and national law and its application to the activities of supervisors at EU and national level and reaching understandings on their respective areas of supervision, in particular concerning EPPO.
- Monitor the implementation of the framework for the interoperability of EU information systems.

3.3 Exchange information and conduct joint audits or coordinated inspections

The Committee will carry out the following tasks under this activity:

- Share information collected on data processing at EU and national levels, and especially on those areas that could present high risks to individual rights.
- Collect information and promote best practices on the engagement with competent authorities at EU and national level.
- Monitor developments and share information on the entry into operation of reforms of existing EU information systems and agencies or creation of new ones.
- Collect and exchange information on the technical implementation of communication systems for exchange of personal data for law enforcement purposes (e.g. SIENA).

¹⁰ Pursuant Article 54(3) of Regulation (EU) 2018/1861 and Article 68(3) of Regulation (EU) 2018/1862.

INTERNAL MARKET INFORMATION SYSTEM (IMI)

- **Provide guidance on the transparency obligations regarding the IMI.**
- **Asses the allocation of roles in terms of controllership within the IMI in relation to the data processed.**
- **Coordinate a supervisory action on how national competent authorities exercise their obligations concerning IMI on management of users' access to the information system for possible joint guidance and/or enforcement at national level.**

EUROPEAN PUBLIC PROSECUTOR'S OFFICE (EPPO)

- **Keep monitoring the implementation of European Delegated Prosecutors' offices at Member State level and the interplay between EPPO and the national databases.**
- **Develop a joint activity between EDPS and national supervisory authorities on the use of case management system of EPPO at Member State level.**

EUROPEAN UNION AGENCY FOR CRIMINAL JUSTICE COOPERATION (EUROJUST)

- **Assess the participation of third country authorities in Joint Investigation Teams under the Eurojust scope and support.**
- **Coordinate a supervisory action at national level on the data quality issues related to data inserted in the Eurojust Counter-Terrorism Register (CTR).**

EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT COOPERATION (EUROPOL)

- **Ensuring the smooth transition from ECB to CSC of ongoing activities and inquire about new possibilities of cooperation and exchange of information between supervisory authorities and law enforcement authorities. This also includes following closely the implementation of the new legal framework, in particular as regards the determination of the purposes of the data processing by the national competent authorities and by Europol.**
- **Inspecting the lawfulness of processing of data on minors sent by national competent authorities to Europol as regards national law and the Europol Regulation, based on prior EDPS referrals and involving the SAs of those Member States concerned.**
- **Addressing the so called "big data challenge" in close cooperation between the EDPS and national SAs, either by checking compliance with national law when data is transmitted to Europol and compliance with the Europol Regulation when data is further processed by Europol. Special attention will be given to the processing of data without data subject categorization.**
- **Monitoring the implementation of the provisions on "information alerts" to be inserted in the SIS by Member States on proposal by Europol, either at national level (SIS) or/and at EU level (Europol), in particular by checking the periodic reporting mechanism in place on those**

alerts. This is the first cross-system supervisory activity covering two EU-systems under the purview of the CSC.

3.4 Prepare the coordinated supervision of EU bodies and information systems that will fall under the Committee's scope

The Committee will carry out the following tasks under this activity:

- **Prepare the Committee's assumption of the coordinated supervision over the EU information systems and agencies that will fall within the scope of the CSC.**
 - Take stock of the relevant undergoing activities of the existing supervision coordination groups.
 - Engage with those groups on specific EU information systems and agencies and with the EDPS, which provides their secretariat, to prepare their transition to the coordinated supervision of the CSC.
- **Ensure the participation of SAs in trainings and joint evaluation missions in relation to the SIS in the framework of a new evaluation mechanism.**

Rules of Procedure of the Coordinated Supervision Committee

Adopted on 3 December 2019

I. The Coordinated Supervision Committee

Article 1 – Identity and Missions

1. The Coordinated Supervision Committee (“the Committee”) is a group of national supervisory authorities and the European Data Protection Supervisor (EDPS). It is established within the framework of the European Data Protection Board (“the Board”), in accordance with Article 37 of the Board’s rules of procedure, to ensure coordinated supervision of large scale IT systems and of EU bodies, offices and agencies in accordance with Article 62 of Regulation (EU) 2018/1725 or with the EU legal act establishing the large scale IT system or the EU body, office or agency.
2. For the purpose of paragraph 1, the Committee shall, as necessary:
 - a) exchange relevant information,
 - b) assist the supervisory authorities in carrying out audits and inspections,
 - c) examine difficulties of interpretation or application of the EU legal act establishing the large-scale IT system or the EU office, body or agency subject to coordinated supervision,
 - d) study problems with the exercise of independent supervision or with the exercise of the rights of data subjects,
 - e) draw up harmonised proposals for solutions to problems and,
 - f) promote awareness of data protection rights.
3. Each authority participating in the Committee shall act within the scope of their respective competences and cooperate actively within the framework of their respective responsibilities to perform the tasks referred to in paragraph 2.

II. Composition

Article 2 – Composition and Participation

1. The Committee shall be composed of the supervisory authorities of each EU Member State and the EDPS, as well as supervisory authorities of non-EU Members of the Schengen Area when foreseen under EU law.
2. The representatives of the national supervisory authorities may participate in the activities of the Committee only when their respective country applies the EU legal act establishing the large scale IT system or the EU office, body or agency.

When ,in accordance with Article 1 and 2 of Protocol No. 22 on the position of Denmark, annexed to the TEU and to the TFEU, Denmark is not bound by the EU legal act establishing the large scale IT system or the EU office, body or agency, Denmark may participate in the activities of the Committee when:

- a) it has implemented the EU legal act, including relevant provisions on coordinated supervision, in its national law, or
 - b) it is bound by way of an agreement that allows for participation in the Committee.
3. Where in a country there is more than one supervisory authority responsible, a joint representative shall be designated. The joint representative may, if necessary in accordance with national procedure, be accompanied by representatives of other supervisory authorities of their country.
4. Where, in accordance with the paragraph 3, there is more than one supervisory authority for a country participating in the activities of the Committee, each country shall cast only one vote.

Article 3 – Appointment of the Coordinator and Deputy Coordinator

1. The Committee, through secret ballot, shall elect a Coordinator and at least one Deputy Coordinator by simple majority.
2. In case the elected Coordinator is a representative of a national supervisory authority of a country that does not apply one or several legal acts in accordance with Article 1, the Committee shall ensure that a Deputy Coordinator is a representative of a national supervisory authority of a country that applies at least such legal act(s).
3. The Coordinator and the Deputy Coordinator(s) shall be designated for a term of two years starting from the date of their respective elections. The Coordinator and the Deputy Coordinator(s) may be re-elected once for a further two years.
4. The term of office of the Coordinator and of the Deputy Coordinator(s) is terminated as soon as the term of office at their supervisory authority ends, or when the two-year term of office ends, or in case of resignation.

Article 4 – Duties of the Coordinator and Deputy Coordinator(s)

1. The Coordinator chairs the Committee meetings in a neutral manner and acts as a contact point in all respective matters.
2. The Coordinator shall:
 - set the draft agenda,
 - convene and chair the meetings of the Committee,
 - carry out all the tasks that have been assigned to him/her in these Rules, and
 - update the Board of the work of the Committee at least twice a year.
3. If the Coordinator is unable to attend, a Deputy Coordinator shall perform the tasks mentioned in paragraphs 1 and 2.

4. The Coordinator shall cooperate with the Deputy Coordinator(s) in liaison with the Secretariat to:
 - a) ensure the smooth functioning of the Committee;
 - b) prepare the draft agenda;
 - c) prepare the draft work program and the draft joint report of activities on coordinated supervision to be adopted by the Committee.
5. The Coordinator and the Deputy Coordinator(s) shall be responsible for the external representation of the Committee.

Article 5 – Experts, guests and other external parties

1. Upon proposal by any participant to the Committee, the Coordinator may, unless a majority of the Committee's participating authorities object, invite via the Secretariat external experts, guests or other external parties to take part in meetings of the Committee and may indicate the topics in the agenda, to which they are invited to attend.
2. The invited experts, guests or other external parties participating in a Committee meeting must be mentioned in the respective agenda and in the minutes.
3. Experts, guests and other external attendants shall be bound by the same confidentiality requirements as the participating authorities of the Committee as provided in Article 21 of these Rules.

III. Documents and procedures

Article 6 – Adoption of reports, guidelines, recommendations and best practices

1. The Committee may adopt reports, guidelines, recommendations and best practices on all matters relating to its tasks, as per Article 1 (2) of these Rules.
2. Except where these Rules provide otherwise, the reports, guidelines, recommendations and best practices of the Committee shall be adopted by consensus. In case where consensus cannot be reached, the reports, guidelines, recommendations and best practices may be adopted by simple majority of authorities participating in the activities in accordance with Article 2.

Article 7 – Written procedure

1. The Coordinator or a majority of the Committee's participating authorities , may decide to submit documents to a written procedure. The Coordinator, via the Secretariat, shall inform participating authorities as soon as possible of the need and the reasons for a written procedure.
2. When a written procedure has been decided, the Secretariat shall send the invitation to start the written procedure to supervisory authorities participating in the activities in accordance with Article 2(2) of these Rules and make the relevant documents available. The participating

authorities may react within one week or another deadline set by the Coordinator, by specifying whether they have formal objections to the document.

3. Unless a participating authority has formally objected to the document subject to the written procedure within the deadline, the document shall be deemed adopted.

Article 8 – Role and responsibilities of Rapporteurs

1. The Committee or the Coordinator may designate one or several (co-) rapporteur(s) for specific issues on a case-by-case basis.
2. The (co-) rapporteur(s) is/are responsible for the elaboration of documents, incorporating comments into revised drafts, finalizing the document and presenting them to the Committee.

Article 9 – Publication of documents

Reports, guidelines, recommendations and documents adopted by the Committee shall be public, unless the Committee decides otherwise.

Article 10 – Joint report of activities on coordinated supervision

1. The Committee shall adopt a joint report of activities on coordinated supervision every two years. That report shall describe the activities of the Committee related to each large scale IT system and EU office, body or agency subject to coordinated supervision. It shall also include a chapter on each country prepared by the participating authority of that country when required by the EU legal act establishing the large-scale IT system or the EU office, body or agency subject to coordinated supervision.

For the coordinated supervision of the Schengen Information System (SIS), as per Article 57 of Regulation 2018/1861 and Article 71 of Regulation 2018/1862, the Committee shall adopt a joint report of activities every year.

2. The joint report of activities on coordinated supervision shall be communicated by the Coordinator to the Board for submission to the European Parliament, the Council and the Commission as well as other addressees when specifically required in the EU legal act establishing the large-scale IT or the EU office, body or agency subject to coordinated supervision.

3. The joint report of activities on coordinated supervision shall also be made available on the Board's website.

Article 11 – Committee work program

The Committee shall adopt a two-year work program.

IV. Working methods

Article 12 – Meetings of the Committee

1. The Committee shall meet at least twice a year.
2. The ordinary meetings shall be convened by the Coordinator not less than three weeks prior to the meeting. The Secretariat shall issue the invitation to each participating authority. Where technically feasible and secure, participants may attend ordinary meetings remotely through videoconferencing or other technical means.
3. Extraordinary meetings may also be convened by the Coordinator, on its own initiative or at the request of the majority of the Committee's participating authorities. Where technically feasible and secure, participants may attend extraordinary meetings remotely through videoconferencing or other technical means.
4. The Coordinator or the Deputy-Coordinator(s) in accordance with Article 4(2) of these Rules, shall direct the proceedings during the meeting.
5. Meetings shall only take place if at least half of the participating authorities or their representatives are attending.

Article 13 – Agenda of meetings

1. Once a meeting has been scheduled, the coordinator should, via the Secretariat, send the Committee a draft agenda without delay and in any event 10 days in advance of the meeting.
2. The draft agenda shall be structured on the basis of the following subject matters:
 - (a) Border, asylum and migration
 - (b) Police and judicial cooperation
 - (c) Digital single market
 - (d) Miscellaneous
3. Participating authorities may propose additional topics to be included as an item on the draft agenda.
4. The draft agenda shall be adopted at the beginning of a meeting.
5. Experts, guests and other external attendants participating in a meeting shall be mentioned in the respective agenda item and discussions point for which they will attend.

Article 14 – Documents for meetings

As a rule, all relevant documents shall be circulated as early as possible via the Secretariat, in any event 10 days in advance of the meeting. In exceptional circumstances, given the importance of the matter or the urgency, documents may be distributed later.

Article 15 – Minutes of meetings

1. After approval by the Coordinator, the Secretariat shall prepare the draft minutes of the Committee's meetings and send them for comments to all participating authorities after the meeting. A list of participants to meetings should appear in annex to the minutes.
2. The draft minutes shall include a summary of the discussions, a record of the conclusions reached and the documents adopted.
3. The draft minutes shall be circulated to the participating authorities for approval.

V. Secretariat and organisation

Article 16 – Convening and venue

1. Committee meetings should be planned well in advance by the Coordinator, together with the Secretariat. The planning of meetings should take into account budgetary constraints.
2. As a general rule, the Committee should meet in person in Brussels. Where possible or necessary, in urgent cases, meetings may take place by way of telecommunication and/or videoconferencing.

Article 17 – Secretariat of the Committee

The Secretariat of the Board shall also provide the Secretariat of the Committee.

Article 18 – Travel costs and reimbursement

One representative of each Member State shall be entitled to the reimbursement of their travel expenses for the participation to the Committee meeting. Representatives from EFTA States shall not be entitled to reimbursement.

Article 19 – Language

The working language of the Committee shall be English.

VI. Final provisions

Article 20 – Access to meetings

Attendance to the Committee meetings is restricted to persons mentioned in Article 2 (Composition and Participation), Article 5 (Experts, guests and other external parties) and Article 17 (Secretariat) of these Rules.

Article 21 – Confidentiality of discussions

Participants to the Committee and the Secretariat shall be obliged to treat in a confidential manner any information that comes to their knowledge in the context of their activities and shall exercise discretion with regard to the discussions of the Committee.

Article 22 – Revision of the Rules of Procedure

1. Amendments to these Rules may be proposed by the Coordinator of the Committee or by one of its participating authority.
2. Amendments shall be adopted in accordance with Article 6(2). These Rules shall be reviewed within two years after their adoption by the Committee.

Article 23 – Webpage of the Committee

The Committee shall have a dedicated webpage on the Board's website.

Article 24 – Entry into force

These Rules shall enter into force on the date of their adoption.

Rules of Procedure for the “Informal Panel of EU DPAs” according to the EU-US Data Privacy Framework

Adopted on 17 April 2024

The “Informal Panel of EU DPAs” (hereinafter: “panel”) is designed according to recital 75 of the Commission Implementing Decision C(2023) 4745 of 10 July 2023 (hereinafter: Data Privacy Framework or DPF) and the supplemental principle III.5 (Operation of DPA Panels) of the Annex II.

The panel is competent for providing binding advice to the US organisations following unresolved DPF complaints from individuals about the handling of personal information that has been transferred from the European Union¹ (hereinafter: EU) under the Data Privacy Framework. The referral to the panel can be made either directly by the individual or by the US company. The panel will seek to deliver advice as quickly as the requirement for due process allows. As a general rule, the panel will aim to provide advice within 60 days after receiving a DPF complaint from an individual or a referral from an organisation concerned. This deadline is indicative and not binding for the DPAs. However, advice will be issued by the panel only after both sides in a dispute have had a reasonable opportunity to comment and to provide any evidence they wish. The advice has the aim to bring the processing activities of personal data transferred under the Data Privacy Framework in line with the DPF. In cases of non-compliance with the advice given by the panel, the panel will refer such cases to the DoC (which may remove organisations from the EU-U.S. DPF list) or, for possible enforcement action, to the FTC or the DoT (failure to cooperate with the DPAs or to comply with the Principles is actionable under U.S. law).²

These rules do not affect the enforcement powers and actions (if any) of the Supervisory Authorities against the exporter and the rights of the data subjects in this respect.

The following rules of procedure will give guidance on how the panel will operate.

For all procedural rules that are not specified in the Data Privacy Framework and in these Rules of Procedure, the DPF complaint/referral will be handled according to the procedural rules of the Member State of the Lead DPA that will adopt the decision.

1. EVALUATION OF THE COMPETENCE OF THE EU PANEL

The Data Protection Authority (hereinafter: DPA) that received a DPF complaint or referral will assess if the panel is competent to handle the DPF complaint or referral.

The panel is only competent for organisations which have committed to cooperate with the DPAs or which process human resources data collected in the context of an employment relationship. The competence of the panel can be verified on the Data Privacy Framework website of the US Department of Commerce³.

¹ References to the EU should be understood as also including the three EEA countries not part of the EU.

² Rec. 73 DPF.

³ One can do this by typing the organisation’s name into the search bar within the Data Privacy Framework List available at <https://www.dataprivacyframework.gov/>, and then by clicking on the organisation’s name, and then on “Questions or DPF complaints?”; where the panel is competent, it is referred to as “EU Data Protection Authorities (DPAs)”.

If the panel is not competent, the DPA that received a DPF complaint/referral will assess if its competence toward the EU data exporter would make it the most appropriate body to handle the DPF complaint or referral and/or will explore possibilities to refer the case to the US Department of Commerce (hereinafter: "DoC") or the US Federal Trade Commission (hereinafter: "FTC")⁴ or the US Department of Transportation (hereinafter: "DoT").

Where the panel is competent, there is a need to designate the lead DPA and co-reviewer DPAs.

2. DESIGNATION OF LEAD-DPA AND CO-REVIEWER DPAS

For the handling of each DPF complaint or referral, the panel will be formed by one DPA acting as lead DPA and other designated co-reviewer DPAs.

The decision on which DPAs will act as lead and as co-reviewers should be taken in a timely manner and should, in principle, be confirmed by the members of the panel within two weeks' time from the receipt of the initial DPF complaint/referral.

Designation of the Lead-DPA

Principle

As a general rule, the lead DPA for handling a DPF complaint within the panel should be the national DPA that receives the DPF complaint by an individual.

As a general rule, the lead DPA for handling a referral by a certified US company should be the national DPA that is competent for the exporter⁵.

If the same or very similar DPF complaints are lodged with several DPAs it will be presumed that the DPA that first received a DPF complaint will act as lead DPA.

Derogations

In exceptional circumstances, another DPA can be designated as lead. This may arise when the DPF complaint concerns a data transfer that relates to a cross-border processing as set out in Art. 4 (23) of the General Data Protection Regulation (GDPR). In such situation, the lead DPA under Article 56 GDPR (i.e. the supervisory authority of the main establishment or of the single establishment of the data exporter) shall decide whether or not it will act as lead DPA also for handling the DPF complaint in the panel.

⁴ Referral to the FTC seems to be only useful for cases that have a systematic character, i.e. cases of systemic failure. This DPA will however also refer cases which, taken together with others, may then point to a failure in an US company's systems and procedures.

⁵ As defined in the EDPB's 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.

Designation of the co-reviewer DPAs

As a general rule, there should be two co-reviewers. In appropriate circumstances the panel can be extended if more than two DPAs are interested in participating in the panel and can put forward a specific interest.

Where the supervisory authority of the main establishment or of the single establishment of the data exporter in the sense of Article 56 as outlined above decides to act as lead DPA, the concerned DPAs (Art. 4 (22) GDPR) should act as co-reviewers.

In cases where fewer than two DPA indicate an interest in acting as co-reviewer, the lead DPA has the prerogative to designate up to two co-Reviewers. When selecting the co-reviewers the lead DPA should in particular take into consideration DPAs in whose jurisdiction the EU headquarter or significant subsidiaries of the US company's group are situated, if any. Other criteria that can be considered include the place where the relevant data processing is facilitated in the EU, the place in the EU from which most data transfers take place, the place where a large number of EU individuals are likely to be affected by the alleged violation, particular expertise located with a certain DPA, and available resources.

The DPAs shall respond to the enquiry to act as co-reviewers from the lead DPA within one week.

3. DUTIES OF DPA THAT RECEIVES A DPF COMPLAINT/REFERRAL

The DPA that receives a complaint from an individual or a referral from a US company shall:

- check if the panel is the competent body for the respective DPF complaint/referral (HR-data collected in the context of an employment relationship, or commitment by the US company to submit to oversight by EU DPAs)
- if this is not the case, forward the complaint to the competent body (e.g . DPA unit responsible for handling DPF complaints under the EU-U.S. Data Privacy Framework in the area of national security, DoC, FTC) and inform complainant/referring company
- if appropriate, encourage and if necessary help complainants in the first instance to use the DPF complaint handling arrangements provided by the companies
- inform all EDPB-members about DPF complaint/referral upon reception
- take all necessary steps for the appointment of the Lead-DPA and the co-reviewers
- provide any translation needed (mostly into and from English or other languages where appropriate) emerging from the communication with the complainant and the DoC, the FTC or any other US statutory body through the panel, regardless of whether the DPA is acting as lead or not.

4. DUTIES OF THE LEAD-DPA

The duties of the lead authority include:

- act as single point of contact for the complainant throughout the entire panel procedure and facilitate communication between and with the panel, regardless of whether the DPA is acting as lead or not
- act as single point of contact towards the US-company concerned respectively the referring company throughout the entire panel procedure and facilitate communication between and with the panel
- identify or designate co-reviewers in consultation with the DPAs
- inform all EDPB -members about the participating DPAs in the panel
- inform the US-organisation in writing of the substance of the DPF complaint and any other relevant information; personal data of the complainant should only be transferred if it is necessary to resolve the DPF complaint
- before any transfer of personal data, inform the data subject and provide them with the opportunity to oppose to the transfer
- offer all sides (complainant, company) reasonable opportunity to comment and to provide any evidence they wish on the matter within a reasonable time-limit
- draft an advice including remedies (where appropriate) and circulate among co-reviewers
- take comments from co-reviewers into consideration and discuss if necessary and endeavour to reach a consensus
- issue the consolidated advice to the US-company
- inform the other EEA DPAs of the advice issued without disclosing the personal data of the individuals and respecting any obligations of commercial confidentiality
- make public the results of the consideration of DPF complaints, if appropriate and by respecting commercial confidentiality duties
- in case of non-compliance by a Data Privacy Framework certified US-company with the advice issued by the panel, prepare a draft on how to proceed given the options mentioned below and coordinate a decision in consultation with the other members of the panel
- if an US-Company fails to comply within 25 days of the delivery of the advice and has offered no satisfactory explanation for the delay, give notice of the panel's intention either to refer the matter to the FTC, DoT, or other US Federal or state body with statutory powers to take enforcement action in cases of deception or misrepresentation, or to conclude that the

agreement to cooperate⁶ has been seriously breached and must therefore be considered null and void and in the latter case, inform the DoC so that the Data Privacy Framework List can be duly amended

- act as single point of contact to FTC, DoC and other relevant public authorities in the US throughout the entire panel procedure and facilitate communication between and with the panel.

5. DUTIES OF CO-REVIEWERS

The duties of the co-Reviewers include:

- support the lead DPA when necessary or requested
- provide comments on the draft advice as quickly as possible and within two weeks maximum to allow for further enquiry; if no comments are provided within this timeframe, it will be considered that the co-reviewers agree with the draft advice prepared by the lead DPA; DPAs might request additional time if necessary and justified.

6. COOPERATION AND COMMUNICATION

Communication between DPAs will be carried out in the framework of the cooperation tools used under Article 57(1)(a), (f) and (g).

The Lead DPA and the co-Reviewer DPAs will work together to reach consensus as to the advice which will be provided to the US company. If there is difficulty in reaching the consensus, as a last resort, a vote may be cast on the existing draft advices. The draft advice that receives the simple majority of the votes of the panel members (Lead DPA and co-reviewer DPAs) will be selected. In case of a tie, the lead DPA's vote will prevail.

The same procedure applies for determining how to proceed in cases of non-compliance by the US-company with the advice issued.

⁶ Supplemental Principle 5, c ii.

EU-US Data Privacy Framework

Template Complaint Form for Submitting Commercial Related Complaints to EU DPAs

Adopted on 17 April 2024

In order to facilitate the handling of your complaint, you should provide your national Data Protection Authority (“DPA”) with the following information. However, please note that the use of this form remains optional and you can choose to contact with your national DPA by other means of communication. Please bear in mind, though, that the information requested in the form below is needed in order to handle your complaint.

1. Please provide the following information:
 - a. Name or other type of identifier used by the US company to individualise you, such as username (mandatory in the case in which the right of access is at stake)¹;
 - b. Preferred contact (i.e. phone number, e-mail address, mailing address);
 - c. Your name (for contact purposes).
2. If known, which company has sent your data to the US? (Please provide contact information related to this company).
3. If known, which is/are the United States companies believed to be involved in processing your personal data?
4. Please elaborate on the reasons why you know/believe that your personal data have been transferred from the EU to a Data Privacy Framework US organisation (for instance, information given on transfers under the Data Privacy Framework in a privacy policy of an EU company processing your personal data)?
5. Please explain the alleged violation of the Data Privacy Framework by the US organisation.
6. If you are looking for information on the processing of your personal data by the US company or relief from an alleged unlawful processing carried out by this entity, please provide some details.
7. Did you already try to resolve your case by contacting the U.S Company (or companies) involved directly?² If yes, what was the outcome? Please provide the previous correspondence in that matter.

¹ If your complaint concerns your right of access to your personal data, it will be necessary to provide this information since otherwise the US company will not know which user has lodged the complaint and hence will not be able to identify and therefore to handle the case. Additional information might also be asked by DPAs to ensure the proper verification of this information (authentication).

² Please note that in most cases, it would be advisable that you first contact the US Data Privacy Framework-certified company to attempt to resolve your case. Your national EU DPA can help you to do so.

8. What other measures have you taken to obtain the information or relief requested and what response have you received through those other measures?

Who will be handling the data provided by this form and how is my personal data protected?

Your DPA is the data controller of personal information provided in the form and will process the personal data in the performance of its tasks carried out in the public interest in accordance with Article 6(1)(e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”) with particular reference to the task referred to in Article 57(1)(a),(f) and (g). Where the “Informal Panel of EU DPAs” is competent³, your personal data will be shared with the EU DPAs participating to the panel. European data protection law applies to protect your personal data processed by all EU DPAs involved and personal data will be stored for the time necessary to process the complaint and in accordance with applicable MS law [see information notice of each SA]. You can exercise your right of access and rectification, erasure or limitation of the processing or to oppose the processing (Articles 15 et seq. GDPR) by contacting, in particular, the data protection authority you lodged the complaint with. In accordance with European data protection law the DPAs will process your personal data exclusively for the purpose of handling your complaint. Your data will be submitted to restricted access and available only to authorised personnel within the relevant DPA.

Will my personal data be transferred to US-companies or to US-authorities?

Where your complaint can be handled without disclosing your personal data, they will not be disclosed in compliance with the principle of data minimisation.

Please be advised that the handling of your complaint might require the transfer of your personal data to the concerned US company and/or US-authorities (US Department of Commerce - DoC, US Federal Trade Commission - FTC, US Federal Transportation Authority - FTA). Such personal data may include your name, any other identifier you have used when communicating with the US-company or any other personal information that has been processed by the US –company and is part of your complaint.

If such transfer turns out to be necessary in order to handle your complaint, you will be specifically informed before the data is transferred and you will be given the opportunity to decide if you wish to proceed.

The outcome of the complaint procedure might be published, if appropriate. However, your personal data will not be disclosed in the course of this publication.

³ The ‘Informal Panel of EU DPAs’ is a group of Data Protection Authorities of EU Member States that will be set up in order to handle a complaint concerning human resources personal data transferred from an EU entity to an US Data Privacy Framework company, or when the US company has voluntarily committed to cooperate with the EU DPAs. See Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, Recital 75.

Statement



Statement 01/2019 on the US Foreign Account Tax Compliance Act (FATCA)

The European Data Protection Board has adopted the following statement:

This statement follows the Resolution passed by the European Parliament on 5 July 2018 on the adverse effects of the US Foreign Account Tax Compliance Act (FATCA) on EU citizens¹ and the requests made by the Association of Accidental Americans to the WP29 in this respect.

European Data Protection Authorities have long been attentive to the data protection issues raised by the automatic exchange of personal data for tax purposes. The Article 29 Working Party (WP29), which preceded the European Data Protection Board, has taken several actions in the past with regards to the automatic exchange of personal data for tax purposes and more specifically with regards to the US Foreign Account Tax Compliance Act (FATCA) in two letters published on 21 June 2012² and on 1 October 2012³. The WP29 also issued a statement on automatic inter-state exchanges of personal data for tax purposes (WP 230 - 4 February 2015) and guidelines for Member States on the criteria to ensure compliance with data protection requirements in the context of the automatic exchange of personal data for tax purposes (WP 234 - 16 December 2015). Finally, the WP29 addressed a letter to the Association of Accidental Americans (8 February 2018)⁴ with regards to the scope of application of the FATCA legislation and relevant data protection issues.

With respect to the European Parliament resolution of 5 July 2018, the European Data Protection Board (EDPB) will pay due attention to the call made to it to review the existing data protection safeguards under the legislation authorising the transfer of personal data to the US IRS for the purposes of the US Foreign Account Tax Compliance Act. It however wishes to highlight that it has initiated work on the preparation of guidelines on some of the tools provided for by Article 46 of the GDPR. More specifically, the guidelines will provide information to interested stakeholders on the elaboration of transfer tools based on Articles 46 (2) (a) and 46 (3) (b) of the GDPR.

¹ [European Parliament resolution of 5 July 2018 on the adverse effects of the US Foreign Account Tax Compliance Act \(FATCA\) on EU citizens and in particular ‘accidental Americans’](#)

² [Letter of the Chair of the ART 29 WP to the Director General of Taxation and Customs Union 21 June 2012](#)

³ [Letter of the Chair of the ART 29 WP to the Director General of Taxation and Customs Union 01 October 2012](#)

⁴ [Letter of the Chair of the ART 29 WP to collective of European “accidental Americans” 08 February 2018](#)

This guidance will include information on the minimum guarantees to be included in legally binding and enforceable instruments concluded between public authorities and bodies (46 (2) (a)) as well as for provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights (46 (3) (b)). It should be noted that legally binding instruments do not require specific authorisation from a supervisory authority whereas the provisions to be included in administrative arrangements are subject to such authorisation from the competent supervisory authority.

This set of guidelines, which should be adopted by the EDPB before the end of 2019, will be a useful tool also for the evaluation of intergovernmental agreements signed between Member States and the US government on FATCA to ensure their compliance with the GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Draft administrative arrangement for the transfer of personal data between

Each of the European Economic Area (“EEA”) Authorities set out in Appendix A

and

Each of the non-EEA Authorities set out in Appendix B

each an “Authority”, together the “Authorities”,

acting in good faith, will apply the safeguards specified in this administrative arrangement (“Arrangement”) to the transfer of personal data between them,

recognizing the importance of the protection of personal data and of having robust data protection regimes in place,

having regard to Article 46(3) (b) of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (“General Data Protection Regulation” or “GDPR”)¹,

having regard to Article 48(3) (b) of the Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (“Regulation 2018/1725”)²,

having regard to the relevant legal framework for the protection of personal data in the jurisdiction of the Authorities and acknowledging the importance of regular dialogue between the EEA Authorities and their national Data Protection Authorities, or the European Data Protection Supervisor (“EDPS”) in the case of the European Securities and Markets Authority (“ESMA”),

having regard to the need to process personal data to carry out the public mandate and exercise of official authority vested in the Authorities, and

having regard to the need to ensure efficient international cooperation between the Authorities acting in accordance with their mandates as defined by applicable laws to safeguard investors or customers and foster integrity and confidence in the securities and derivatives markets,

have reached the following understanding:

¹ OJ L119/1, 04/05/2016

² OJ L295/39, 21/11/2018

I. Purpose and Scope

This Arrangement is limited to transfers of personal data between an EEA Authority set out in Appendix A and a non-EEA Authority set out in Appendix B, in their capacity as public Authorities, regulators and/or supervisors of securities and/or derivatives markets.

The Authorities are committed to having in place appropriate safeguards for the processing of such personal data in the exercise of their respective regulatory mandates and responsibilities.

Each Authority confirms that it can and will act consistent with this Arrangement and that it has no reason to believe that existing applicable legal requirements prevent it from doing so.

This Arrangement is intended to supplement existing information sharing arrangements or memoranda that may exist between one or more EEA Authorities and one or more non-EEA Authorities, and to be applicable in different contexts, including information that may be shared for supervisory or enforcement related purposes.

While this Arrangement is specifically intended to provide safeguards for personal data transfers, it is not the only means by which personal data may be transferred, nor does it prohibit an Authority from transferring personal data pursuant to a relevant agreement, another relevant arrangement, or a process separate to this Arrangement, for example pursuant to an applicable adequacy decision.

Effective and enforceable data subject rights are available to Data Subjects under applicable legal requirements in the jurisdiction of each Authority, however this Arrangement does not create any legally binding obligations, confer any legally binding rights, nor supersede domestic law. The Authorities have implemented, within their respective jurisdictions, the safeguards set out in Section III of this Arrangement in a manner consistent with applicable legal requirements. Authorities provide safeguards to protect personal data through a combination of laws, regulations and their internal policies and procedures.

II. Definitions

For the purposes of this Arrangement:

- (a) “**applicable legal requirements**” means the relevant legal framework for the protection of personal data applicable to each Authority;
- (b) “**criminal data**” means personal data relating to criminal convictions and offences or related security measures;
- (c) “**onward transfer**” means the transfer of personal data by a receiving Authority to a third party in another country who is not an Authority participating in this Arrangement and when that transfer is not covered by an adequacy decision from the European Commission;
- (d) “**personal data**” means any information relating to an identified or identifiable natural person (“Data Subject”) within the scope of this Arrangement; 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;

- (e) "**personal data breach**" means a breach of data security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- (f) "**processing**" means any operation or set of operations performed on 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;
- (g) "**professional secrecy**" means the general legal obligation of an Authority not to disclose non-public information received in an official capacity;
- (h) "**profiling**" means automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person;
- (i) **GDPR Data Subject Rights:** The GDPR generally provides the following Data Subject Rights:
 - i. "**right not to be subject to automated decisions, including profiling**" means a Data Subject's right not to be subject to legal decisions being made concerning him or her based solely on automated processing;
 - ii. "**right of access**" means a Data Subject's right to obtain from an Authority confirmation as to whether or not personal data concerning him or her are being processed, and where that is the case, to access the personal data;
 - iii. "**right of erasure**" means a Data Subject's right to have his or her personal data erased by an Authority where the personal data are no longer necessary for the purposes for which they were collected or processed, or where the data have been unlawfully collected or processed;
 - iv. "**right of information**" means a Data Subject's right to receive information on the processing of personal data relating to him or her in a concise, transparent, intelligible and easily accessible form;
 - v. "**right of objection**" means a Data Subject's right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her by an Authority, except in cases where there are compelling legitimate grounds for the processing that override the grounds put forward by the Data Subject or for the establishment, exercise or defence of legal claims;
 - vi. "**right of rectification**" means a Data Subject's right to have the Data Subject's inaccurate personal data corrected or completed by an Authority without undue delay;
 - vii. "**right of restriction of processing**" means a Data Subject's right to restrict the processing of the Data Subject's personal data where the personal data are inaccurate, where the processing is unlawful, where the Authority no longer needs the personal data for the purposes for which they were collected or where the personal data cannot be deleted;

- (j) “**sharing of personal data**” means the sharing of personal data by a receiving Authority with a third party in its country, or in the case of ESMA the sharing of personal data with a third party within the jurisdictions of the EEA Authorities.

III. Personal data protection safeguards

1. **Purpose limitation:** The Authorities have regulatory mandates and responsibilities which include protecting investors or customers and fostering integrity and confidence in securities and/or derivatives markets. Personal data are transferred between the Authorities to support these responsibilities and are not transferred for other purposes such as for marketing or commercial reasons.

The transferring Authority will transfer personal data only for the legitimate and specific purpose of assisting the receiving Authority to fulfil its regulatory mandate and responsibilities, which include regulating, administering, supervising, enforcing and securing compliance with the securities or derivatives laws in its jurisdiction. The receiving Authority will not further process the personal data in a manner that is incompatible with these purposes, nor with the purpose that may be set out in any request for the information.

2. **Data quality and proportionality:** The transferring Authority will only transfer personal data that are adequate, relevant and limited to what is necessary for the purposes for which they are transferred and further processed.

The transferring Authority will ensure that to the best of its knowledge the personal data that it transfers are accurate and, where necessary, up to date. Where an Authority becomes aware that personal data it has transferred to, or received from, another Authority is incorrect, it will advise the other Authority about the incorrect data. The respective Authorities will, having regard to the purposes for which the personal data have been transferred and further processed, supplement, erase, block, correct or otherwise rectify the personal data, as appropriate.

3. **Transparency:** Each Authority will provide general notice to Data Subjects about: (a) how and why it may process and transfer personal data; (b) the type of entities to which such data may be transferred; (c) the rights available to Data Subjects under the applicable legal requirements, including how to exercise those rights; (d) information about any applicable delay or restrictions on the exercise of such rights, including restrictions that apply in the case of cross-border transfers of personal data; and (e) contact details for submitting a dispute or claim.

This notice will be effected by the publishing of this information by each Authority on its website along with this Arrangement.

Individual notice will be provided to Data Subjects by EEA Authorities in accordance with notification requirements and applicable restrictions in the GDPR and the national legal framework applicable in the jurisdiction of the EEA Authorities, or in the case of ESMA in accordance with Regulation 2018/1725 as may be further amended, repealed or replaced.

4. Security and confidentiality: Each receiving Authority will have in place appropriate technical and organisational measures to protect personal data that are transferred to it against accidental or unlawful access, destruction, loss, alteration, or unauthorised disclosure. Such measures will include appropriate administrative, technical and physical security measures. These measures may include, for example, marking information as personal data, restricting who has access to personal data, providing secure storage of personal data, or implementing policies designed to ensure personal data are kept secure and confidential.

In the case where a receiving Authority becomes aware of a personal data breach, it will inform the transferring Authority as soon as possible and use reasonable and appropriate means to remedy the personal data breach and minimize the potential adverse effects.

5. Safeguards Relating to GDPR Data Subject Rights:

The Authorities will apply the following safeguards to personal data transferred under this Arrangement:

The Authorities will have in place appropriate measures which they will follow, such that, upon request from a Data Subject, an Authority will (1) identify any personal data it has transferred to another Authority pursuant to this Arrangement, (2) provide general information, including on an Authority's website, about safeguards applicable to transfers to other Authorities, and (3) provide access to the personal data and confirm that the personal data are complete, accurate and, if applicable, up to date.

Each Authority will allow a Data Subject who believes that his or her personal data are incomplete, inaccurate, outdated or processed in a manner that is not in accordance with applicable legal requirements or consistent with the safeguards set out in this Arrangement to make a request directly to such Authority for any rectification, erasure, restriction of processing, or blocking of the data.

Each Authority, in accordance with the applicable legal requirements, will address in a reasonable and timely manner a request from a Data Subject concerning the rectification, erasure, restriction of processing or objection to processing of his or her personal data. An Authority may take appropriate steps, such as charging reasonable fees to cover administrative costs or declining to act on a request, where a Data Subject's requests are manifestly unfounded or excessive.

Each Authority may use automated means to more effectively fulfil its mandate. However, no Authority will take a legal decision concerning a Data Subject based solely on automated processing of personal data, including profiling, without human involvement.

Safeguards relating to GDPR Data Subject Rights are subject to an Authority's legal obligation not to disclose confidential information pursuant to professional secrecy or other legal obligations. These safeguards may be restricted to prevent prejudice or harm to supervisory or enforcement functions of the Authorities acting in the exercise of the official authority vested in them, such as for the monitoring or assessment of compliance with applicable laws or prevention or investigation of suspected offenses; for important objectives of general public interest, as recognised in the jurisdiction of the receiving Authority and, where necessary under the applicable legal requirements, of the

transferring Authority, including in the spirit of reciprocity of international cooperation; or for the supervision of regulated individuals and entities. The restriction should be necessary and provided by law, and will continue only for as long as the reason for the restriction continues to exist.

6. Onward transfers and sharing of personal data:

6.1 Onward transfer of personal data

An Authority receiving personal data pursuant to this Arrangement will only onward transfer the personal data to a third party with the prior written consent of the transferring Authority, and if the third party provides appropriate assurances that are consistent with the safeguards in this Arrangement.

6.2 Sharing of personal data

- (1) An Authority receiving personal data pursuant to this Arrangement will only share the personal data with the prior written consent of the transferring Authority, and if the third party provides appropriate assurances that are consistent with the safeguards in this Arrangement.
- (2) Where assurances contemplated under the first paragraph cannot be provided by the third party, the personal data may be shared with the third party in exceptional cases if sharing the personal data is for important reasons of public interest, as recognised in the jurisdiction of the receiving Authority and, where necessary under the applicable legal requirements, of the transferring Authority, including in the spirit of reciprocity of international cooperation, or if the sharing is necessary for the establishment, exercise or defense of legal claims.
- (3) Where sharing of personal data is for the purpose of conducting a civil or administrative enforcement proceeding, assisting in a self-regulatory organization's surveillance or enforcement activities, assisting in a criminal prosecution, or conducting any investigation for any general charge applicable to the violation of the provision specified in the request where such general charge pertains to a violation of the laws and regulations administered by the receiving Authority, including enforcement proceedings which are public, a receiving Authority may share personal data with a third party (such as public bodies, courts, self-regulatory organizations and participants in enforcement proceedings) without requesting consent from the transferring Authority, nor obtaining assurances, if the sharing is for purposes that are consistent with the purpose for which the data were initially transferred or with the general framework of the use stated in the request, and is necessary to fulfil the mandate and responsibilities of the receiving Authority and/or the third party. When sharing personal data received under this Arrangement with a self-regulatory organisation, the receiving Authority will ensure that the self-regulatory organization is able and will comply on an ongoing basis with the confidentiality protections set forth in Section III (4) of this Arrangement.
- (4) A receiving Authority may share personal data with a third party without requesting consent from the transferring Authority, nor obtaining assurances, in a situation where the sharing of personal data follows a legally enforceable demand or is required by law. The receiving Authority will notify the transferring Authority prior to the sharing and include information about the data requested, the requesting body and the legal

basis for sharing. The receiving Authority will use its best efforts to limit the sharing of personal data received under this Arrangement, in particular through the assertion of all applicable legal exemptions and privileges.

7. **Limited data retention period:** The Authorities will retain personal data for no longer than is necessary and appropriate for the purpose for which the data are processed. Such retention period will comply with the applicable laws, rules and/or regulations governing the retention of such data in the jurisdiction of the receiving Authority.
8. **Redress:** Each Authority acknowledges that a Data Subject who believes that an Authority has failed to comply with the safeguards as set forth in this Arrangement, or who believes that his or her personal data have been subject to a personal data breach, may seek redress against that Authority to the extent permitted by applicable legal requirements. This redress may be exercised before any competent body, which may include a court, in accordance with the applicable legal requirements of the jurisdiction where the alleged non-compliance with the safeguards in this Arrangement occurred. Such redress may include monetary compensation for damages.

In the event of a dispute or claim brought by a Data Subject concerning the processing of the Data Subject's personal data against the transferring Authority, the receiving Authority or both Authorities, the Authorities will inform each other about any such disputes or claims, and will use best efforts to settle the dispute or claim amicably in a timely fashion.

If an Authority or the Authorities are not able to resolve the matter with the Data Subject, the Authorities will use other methods by which the dispute could be resolved unless the Data Subject's requests are manifestly unfounded or excessive. Such methods will include participation in non-binding mediation or other non-binding dispute resolution proceedings initiated by the Data Subject or by the Authority concerned. Participation in such mediation or proceedings may be done remotely (such as by telephone or other electronic means).

If the matter is not resolved through cooperation by the Authorities, nor through non-binding mediation or other non-binding dispute resolution proceedings, the receiving Authority will report this to the assessment group and to the transferring Authority, as outlined in Section IV of this Arrangement. In situations where a Data Subject raises a concern and a transferring Authority is of the view that a receiving Authority has not acted consistent with the safeguards set out in this Arrangement, a transferring Authority will suspend the transfer of personal data under this Arrangement to the receiving Authority until the transferring Authority is of the view that the issue is satisfactorily addressed by the receiving Authority, and will inform the Data Subject thereof.

IV. Oversight

1. Each Authority will conduct periodic reviews of its own policies and procedures that implement this Arrangement and of their effectiveness, the results of which will be communicated to the assessment group described in paragraph IV (4) below. Upon reasonable request by another Authority, an Authority will review its personal data processing policies and procedures to ascertain and confirm that the safeguards in this Arrangement are being implemented effectively. The results of the review will be communicated to the Authority that requested the review.

2. In the event that a receiving Authority is unable to effectively implement the safeguards in this Arrangement for any reason, it will promptly inform the transferring Authority and the assessment group described in paragraph IV (4) below, in which case the transferring Authority will temporarily suspend the transfer of personal data under this Arrangement to the receiving Authority until such time as the receiving Authority informs the transferring Authority that it is again able to act consistent with the safeguards.
3. In the event that a receiving Authority is not willing or able to implement the outcome of the non-binding mediation or other non-binding dispute resolution proceeding referred to in Section III (8) of this Arrangement, it will promptly inform the transferring Authority and the assessment group described in paragraph IV (4) below.
4. An assessment group (“Assessment Group”) established as a sub-committee of the Authorities by the International Organization of Securities Commissions (“IOSCO”) will conduct periodic reviews on implementation of the safeguards in this Arrangement, and will consider best practices with a view to continuing to enhance the protections of personal data where appropriate. Following notice and opportunity to be heard, if the Assessment Group determines that there has been a demonstrated change in the willingness or ability of an Authority to act consistent with the provisions of this Arrangement, the Assessment Group will inform all other Authorities thereof. For purposes of its review, the Assessment Group will have due regard to the information provided by a receiving Authority not being willing or able to implement the outcome of the non-binding mediation or other non-binding dispute resolution proceeding referred to in Section III (8) of this Arrangement. Personal data pertaining to Data Subjects involved in any such proceedings will in principle be anonymized before being provided to the Assessment Group. In addition, the Assessment Group may develop recommendations with respect to the enhancement of the Authority’s policies and procedures for the protection of personal data.
5. The Assessment Group will make written recommendations to an Authority where the Assessment Group finds material deficiencies in the policies and procedures that the Authority has in place to implement the safeguards. If the Assessment Group determines that material deficiencies are not being addressed and that there has been a demonstrated change in the willingness or ability of the Authority to act consistent with this Arrangement, following notice and an opportunity to be heard, it may recommend to the AA Decision Making Group (“AA DMG”) that the Authority’s participation in this Arrangement be discontinued. Any decision of the AA DMG may be appealed by an Authority or by the Assessment Group to the IOSCO Board members that are Authorities.
6. In situations where a transferring Authority is of the view that a receiving Authority has not acted consistent with the safeguards set out in this Arrangement, a transferring Authority will suspend the transfer of personal data to the receiving Authority under this Arrangement until the issue is satisfactorily addressed by the receiving Authority. In the event that a transferring Authority suspends the transfer of personal data to a receiving Authority under this paragraph IV (6) or under paragraph IV (2) above, or resumes transfers after any such suspension, it will promptly inform the Assessment Group, which will in turn inform all other Authorities.

V. Revision and discontinuation

1. The Authorities may consult and revise by mutual consent the terms of this Arrangement in the event of substantial change in the laws, regulations or practices affecting the operation of this Arrangement.
2. An Authority may discontinue its participation in this Arrangement, vis-à-vis another Authority or Authorities, at any time. It should endeavour to provide 30 days' written notice to the other Authority or Authorities of its intent to do so. Any personal data already transferred pursuant to this Arrangement will continue to be treated consistent with the safeguards provided in this Arrangement.
3. The European Data Protection Board ("EDPB"), or the EDPS in the case of ESMA, will be notified by IOSCO of any proposed material revisions to, or discontinuation of, this Arrangement.

Date:

Information note on BCRs for companies which have ICO as BCR Lead Supervisory Authority

Adopted on 12 February 2019

In the event of a No-deal Brexit and the ICO no longer has a role in the BCR community, companies are therefore invited to consider the following:

- Groups headquartered in the UK wishing to apply for BCRs: such Groups should identify the most appropriate BCR Lead Supervisory Authority in a EU Member State, according to the criteria laid down in 1.2 of [WP 263](#).
- Current Applications: Groups for which BCRs are at the review stage by the ICO need to identify a new BCR Lead Supervisory Authority according to the criteria laid down in [WP263](#). The new BCR Lead Supervisory Authority will take over the application and formally initiate a new procedure at the time of a no deal Brexit.

Draft BCRs submitted to EDPB: if a draft ICO decision for approving BCRs is pending before the EDPB at the time of a No-deal Brexit, the Group needs to identify a new BCR Lead Supervisory Authority according to the criteria laid down in [WP263](#). The new BCR Lead will take over and re-submit a draft decision for the approval the BCRs to the EDPB.

- Authorised BCR holders: BCR holders need to identify the new BCR Lead Supervisory Authority, according to the criteria laid down in [WP 263](#).

In any of the above scenarios, the Supervisory Authority that may be approached to act as the new BCR Lead Supervisory Authority will consider in cooperation with other concerned Supervisory Authorities whether it is the appropriate BCR Lead on a case by case basis and inform the Group accordingly. For any questions or further information, Groups are invited to contact the ICO.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Information note on data transfers under the GDPR in the event of a no-deal Brexit

Adopted on 12 February 2019
Updated on 4 October 2019

Introduction

In the absence of an agreement between the EEA and the UK (no-deal Brexit), the UK will become a third country from 00.00 am CET on 1st November 2019. This means that the transfer of personal data to the UK has to be based on one of the following instruments¹ as of 1st November 2019:

- Standard or ad hoc Data Protection Clauses
- Binding Corporate Rules
- Codes of Conduct and Certification Mechanisms
- Derogations²

This note provides information to commercial and public organisations on these transfer instruments under the GDPR for the transfer of personal data to the UK in the event of a no-deal Brexit

The EDPB builds upon the guidance provided on this matter by supervisory authorities and by the [European Commission \(EC\)](#). EEA organisations may turn, if necessary, to the [national supervisory authorities](#) competent to oversee the related processing activities.

¹ See Chapter V of GDPR.

² These can be used only in the absence of Standard Data Protection Clauses or other alternative appropriate safeguards.

I. 5 steps organisations should take to prepare for a no-deal Brexit

When transferring data to the UK, you should:

- 1 • Identify what processing activities will imply a personal data transfer to the UK
- 2 • Determine the appropriate data transfer instrument for your situation (see below)
- 3 • Implement the chosen data transfer instrument to be ready for 1st November 2019
- 4 • Indicate in your internal documentation that transfers will be made to the UK
- 5 • Update your privacy notice accordingly to inform individuals

II. Data transfers from the EEA to the UK

1. Available transfer instruments

In the absence of an adequacy decision³ at the time of the Brexit, the following are the available data transfer instruments.

a. Standard and ad hoc Data Protection Clauses

You and your UK counterpart may agree on the use of Standard Data Protection Clauses approved by the European Commission. These contracts offer the additional adequate safeguards with respect to data protection that are needed in case of a transfer of personal data to any third country.

³ An adequacy decision is a decision adopted by the European Commission on the basis of article 45 GDPR (for example, the adequacy decision on Japan adopted by the Commission on 23rd January 2019. Previously, the EC had also adopted adequacy decisions on third countries such as Argentina, New Zealand and Israel, amongst others). At the moment, there is no such an adequacy decision in place for the UK.

Three sets of Standard Data Protection Clauses are currently available:

- EEA controller to third country (e.g. UK) controller: 2 sets are available:
 - [2001/497/EC](#)
 - [2004/915/EC](#)
- EEA controller to third country (e.g. UK) processor
 - [2010/87/EU](#)

It is important to note that the Standard Data Protection Clauses may not be modified and must be signed as provided. However, these contracts may be included in a wider contract and additional clauses might be added provided that they do not contradict, directly or indirectly, the Standard Data Protection Clauses adopted by the European Commission. Considering the timeframe before the 1st November 2019, the EDPB acknowledges that the Standard Data Protection Clauses is a ready-to-use instrument.

Any further modifications to the Standard Data Protection Clauses will imply that this will be considered as ad-hoc contractual clauses. This can provide appropriate safeguards taking into account your particular situation.

Prior to any transfer, these tailored contractual clauses must be authorised by the competent national supervisory authority, following an opinion of the EDPB.

b. Binding Corporate Rules

Binding Corporate Rules are personal data protection policies adhered to by group of undertakings (i.e. multinationals) in order to provide appropriate safeguards for transfers of personal data within the group, including outside of the EEA.

You may have already in place BCRs or cooperate with processors which make use of BCRs for Processors. Organisations may still rely on these BCRs authorised under the former Directive 95/46/EC which remain valid under the GDPR⁴. These BCRs need however to be updated to be fully in line with the GDPR provisions.

If you do not have BCRs in place, they must be approved by the competent national supervisory authority, following an opinion of the EDPB.

You can find further explanations on the conditions to apply for Binding Corporate Rules on the [EDPB website](#).

⁴ According to article 46.5 GDPR. Please note that BCRs authorised under former Directive 95/46/EC remained valid under the GDPR, but need to be updated to be fully in line with GDPR provisions.

c. Codes of conduct and certification mechanisms

A code of conduct or a certification mechanism can offer appropriate safeguards for transfers of personal data if they contain binding and enforceable commitments by the organisation in the third country for the benefit of the individuals.

These tools are new under the GDPR and the EDPB is working on guidelines in order to give more explanations on the harmonized conditions and procedure for using these tools.

2. Derogations

It is important to underline that the derogations allow the data transfers under certain conditions and are exceptions to the rule of having put in place appropriate safeguards (see the above mentioned instruments like BCRs, standard data protection clauses...) or transfer the data on the basis of an adequacy decision. They must therefore be interpreted restrictively and mainly relate to processing activities that are occasional and non-repetitive.

These derogations include amongst others according to article 49 GDPR:

- where an individual has explicitly consented to the proposed transfer after having been provided with all necessary information about the risks associated with the transfer;
- where the transfer is necessary for the performance or the conclusion of a contract between the individual and the controller or the contract is concluded in the interest of the individual;
- if the data transfer is necessary for important reasons of public interest;
- if the data transfer is necessary for the purposes of compelling legitimate interests of the organisation.

You can find further explanations on available derogations and how to apply them in the [EDPB Guidelines on Article 49 of GDPR](#).

3. Instruments exclusively available to public authorities or bodies

Public authorities may consider to use the mechanisms which the GDPR considers more appropriate to their situation.

One option is to use a legally binding and enforceable instrument, such as an administrative agreement, a bilateral or multilateral international agreement. The agreement must be binding and enforceable for the signatories.

The second option is to use administrative arrangements, such as Memoranda of Understanding, which although not legally binding must however provide for enforceable and effective data subject rights. The administrative arrangements are subject to an authorisation by the competent national supervisory authority, following an opinion of the EDPB.

⁵ See recital 113 and article 49.1 GDPR

In addition, the abovementioned derogations are also available for transfers by public authorities, subject to the application of the relevant conditions.

For public authorities exercising criminal law enforcement functions⁶, additional transfer tools are available⁷.

III. Data transfers from the UK to EEA Members

According to the UK Government, the current practice, which permits personal data to flow freely from the UK to the EEA, will continue in the event of a no-deal Brexit⁸.

To this end, the UK Government's and the ICO's website should be regularly consulted.

For the European Data Protection Board
The Chair

(Andrea Jelinek)

⁶Which fall under the scope of the Law Enforcement Directive.

⁷ See Article 37 and 38 LED. For instance, transfers may take place when the EU authority concludes that appropriate safeguards exist in the third country following a (self-)assessment of all circumstances surrounding the transfer. Moreover, additional derogations for specific situations may be applicable (see Article 38 LED).

⁸[https://www.gov.uk/government/publications/data-protection-if-theres-no-brexit-deal](https://www.gov.uk/government/publications/data-protection-if-theres-no-brexit-deal/data-protection-if-theres-no-brexit-deal)

Work program



EDPB Work Program 2019/2020

The European Data Protection Board

The European Data Protection Board (EDPB) is an independent European body, which contributes to the consistent application of data protection rules throughout the European Union, and promotes cooperation between the EU and EEA EFTA data protection supervisory authorities. The EDPB is established by the General Data Protection Regulation (GDPR).

The EDPB is composed of representatives of the national EU and EEA EFTA data protection supervisory authorities, and the European Data Protection Supervisor (EDPS).

The EDPB has the following main tasks:

- To issue opinions, guidelines, recommendations and best practices to promote a common understanding of the GDPR and the Law Enforcement Directive;
- To advise the European Commission on any issue related to the protection of personal data in the Union;
- To contribute to the consistent application of the GDPR, in particular in cross-border data protection cases
- To promote cooperation and the effective exchange of information and best practice between national supervisory authorities

In line with the Article 29 of the EDPB Rules of procedure, the EDPB has developed its two-year work program for 2019 and 2020. After having endorsed guidelines adopted by the WP29 and after having issued guidelines on the interpretation of the new provisions introduced by the GDPR, the EDPB now aims to focus more on specific items or technologies. The work program of the EDPB is based on the needs identified by the members as priority for stakeholders as well as the EU legislator planned activities.

The EDPB will regularly monitor the implementation of its work program which might be updated.

Activities for 2019-2020

I. Guidelines

- Guidelines on Codes of Conduct and Monitoring Bodies
- Guidelines on delisting
- Guidelines on PSD2 and GDPR
- Guidelines on international transfers between public bodies for administrative cooperation purposes
- Guidelines Certification and Codes of Conduct as a tool for transfers
- Guidelines on Connected vehicles
- Guidelines on Certification (finalisation after the public consultation)
- Guidelines on video surveillance
- Guidelines on Data Protection by Design and by Default
- Guidelines on Targeting of social media users
- Guidelines on children's data
- Guidelines on reliance on Art. 6(1) b in the context of online services
- Guidelines on concepts of controller and processor (Update of the WP29 Opinion)
- Guidelines on the notion of legitimate interest of the data controller (Update of the WP29 Opinion)
- Guidelines on the Territorial Scope of the GDPR (finalisation after the public consultation)
- Guidelines on the powers of DPAs in accordance with Art. 47 of the Law Enforcement Directive
- Guidelines on data subjects rights with main focus at a first stage on the rights of access, erasure, objection, restriction and limitations to these rights

II. Consistency opinions

- Opinion on administrative arrangement between EEA and non EEA financial market regulators
- Opinion on Interplay between GDPR and ePrivacy

III. Other types of activities

- Privacy Shield - Follow-up of the Joint Review
- ePrivacy Regulation
- Procedural rules on the Supervision of EU large scale IT systems
- Consultation from the Commission on the Clinical Trials Regulation
- Reflection paper on international mutual assistance and other cooperation tools to enforce the GDPR outside the EU (Art. 50)
- EDPB Enforcement Strategy
- FATCA - Statement in response to the European Parliament's resolution
- Statement on the use of personal data in the context of elections
- Enhancement of existing IT solutions and development of new IT solutions
- Data breach notifications
- Consultation from the Commission on the report regarding the evaluation and review of the GDPR according to Art. 97

IV. Recurrent activities

a. Consistency opinions and decisions

- Opinions regarding relevant draft decision from competent supervisory authorities, such as decisions on
 - DPIA lists (Art. 35(4)-(5))
 - Codes of conduct
 - Accreditation criteria for code monitoring and certification bodies and certification criteria under Art. 42(5) (European Data Protection Seal)
 - Standard contractual clauses for international transfers under Art. 46(2)
 - Standard contractual clauses for processors under Art. 28(8)
 - Ad hoc contractual clauses for international transfers under Art. 46(3)
 - Binding Corporate Rules (Art. 47(1))
- Any opinion on matter of general application or producing effects in several member States, on the basis of a request from any supervisory authority, the Chair or the Commission under Art. 64(2)
- Any binding decision in the context of dispute resolution (Art. 65(1)) or urgency procedure (Art. 66)

b. Legislative consultation

- Any opinion, statement, advice on the request of the Commission following the adoption of proposals for a legislative act, international agreement or when preparing delegated acts or implementing acts, where the act is of particular importance for the protection of individuals' rights and freedoms with regard to the processing of personal data, such as opinions on future or review of existing Adequacy decisions

V. Possible topics

- Guidelines on the interpretation of Art. 48 GDPR
- Guidance on the interaction between the Regulation on the free flow of non-personal data in the EU and the GDPR
- Opinion on cross-border requests for e-evidence
- Comments on updated PNR agreement with Canada
- Update of guidance on government access to data both in Essential Guarantees paper and Adequacy Referential
- Enforcement against controllers in 3rd countries
- e-Invoices and creation of centralized databases by Ministries of Finance
- Use of credit cards for distant payments and post-transaction retention of card numbers
- Good practices regarding research projects
- Approval procedure for ad hoc contractual clauses
- Blockchain
- Interoperability between BCRs
- Use of new technologies, such as AI, connected assistants

Statement



Statement 2/2019 on the use of personal data in the course of political campaigns

Adopted on 13 March 2019

The European Data Protection Board has adopted the following statement:

Engaging with voters is inherent to the democratic process. It allows the preparation of political programmes, enables citizens to influence politics and the development of campaigns in line with citizens expectations.

Political parties, political coalitions and candidates increasingly rely on personal data and sophisticated profiling techniques to monitor and target voters and opinion leaders. In practice, individuals receive highly personalised messages and information, especially on social media platforms, on the basis of personal interests, lifestyle habits and values.

Predictive tools are used to classify or profile people's personality traits, characteristics, mood and other points of leverage to a large extent, allowing assumptions to be made about deep personality traits, including political views and other special categories of data. The extension of such data processing techniques to political purposes poses serious risks, not only to the rights to privacy and to data protection, but also to trust in the integrity of the democratic process. The Cambridge Analytica revelations illustrated how a potential infringement of the right to protection of personal data could affect other fundamental rights, such as freedom of expression and freedom to hold opinions and the possibility to think freely without manipulation.

The EDPB observes that, in addition to political parties and candidates, several other actors can be involved in the processing of personal data for political purposes: social media

platforms, interest groups, data brokers, analytics companies, ad networks. These actors can play an important role in the election process and their compliance is subject to supervision by independent data protection authorities.

In light of the elections to the European Parliament and other elections in the EU scheduled for 2019, the EDPB wishes to underline a number of key points to be respected when political parties process personal data in the course of electoral activities:

1. Personal data revealing political opinions is a special category of data under the GDPR. As a general principle, the processing of such data is prohibited and is subject to a number of narrowly-interpreted conditions, such as the explicit, specific, fully informed, and freely given consent of the individuals.¹
2. Personal data which have been made public, or otherwise been shared by individual voters, even if they are not data revealing political opinions, are still subject to, and protected, by EU data protection law. As an example, using personal data collected through social media cannot be undertaken without complying with the obligations concerning transparency, purpose specification and lawfulness.
3. Even where the processing is lawful, organisations need to observe their other duties pursuant to the GDPR, including the duty to be transparent and provide sufficient information to the individuals who are being analysed and whose personal data are being processed, whether data has been obtained directly or indirectly. Political parties and candidates must stand ready to demonstrate how they have complied with data protection principles, especially the principles of lawfulness, fairness and transparency.
4. Solely automated decision-making, including profiling, where the decision legally or similarly significantly affects the individual subject to the decision, is restricted. Profiling connected to targeted campaign messaging may in certain circumstances cause ‘similarly significant effects’ and shall in principle only be lawful with the valid explicit consent of the data subject.²
5. In case of targeting, adequate information should be provided to voters explaining why they are receiving a particular message, who is responsible for it and how they can exercise their rights as data subjects. In addition, the Board notes that, under the

¹ See article 9 GDPR. One example is that of data manifestly made public by the data subject, which, like other derogations of special data categories, should be interpreted narrowly, as it cannot be used to legitimate inferred data.

² The EDPB has previously clarified that a legal effect generated by automated decision-making may include affecting a person's vote in an election.

law of some Member States, there is a transparency requirement as to payments for political advertisement.

The EDPB refers political parties and other stakeholders to the practical guidance and recommendations issued by several data protection authorities regarding the use of data in the course of elections.³ It also welcomes the set of measures presented by the European Commission in September 2018,⁴ and the Conclusions of the Council and of the Member States on securing free and fair European elections.⁵

EDPB members also work together with other relevant competent authorities⁶ to ensure consistent interpretation and compliance with applicable laws, including the GDPR, to safeguard trust in the security and integrity of the elections to the European Parliament and other elections in the EU scheduled for 2019 and beyond.

Compliance with data protection rules, including in the context of electoral activities and political campaigns, is essential to protect democracy. It is also a means to preserve the trust and confidence of citizens and the integrity of elections. Ahead of the upcoming electoral deadlines, data protection authorities are committed to monitor and, if necessary, enforce the application of data protection principles in the context of elections and political campaigns, such as transparency, purpose limitation, proportionality and security, as well as the exercise of data subject rights. Data protection authorities will make full use of their powers, as provided by the GDPR, and ensure cooperation and consistency in their actions within the framework of the EDPB.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

³ See Annex I.

⁴ And especially the Guidance on the application of EU data protection law and the Recommendation on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-elections-recommendation-5949_en.pdf.

⁵ <https://data.consilium.europa.eu/doc/document/ST-6573-2019-REV-1/en/pdf>.

⁶ For instance, in the framework of European election networks as further described in the Commission's "electoral package" (see, in particular, the Recommendation on election cooperation networks mentioned in footnote 4 above and the Commission's proposal for a regulation of the European Parliament and of the Council amending Regulation (EU, Euratom) No 1141/2014 as regards a verification procedure related to infringements of rules on the protection of personal data in the context of elections to the European Parliament).

ANNUAL REPORT 2024

PROTECTING PERSONAL DATA IN A CHANGING LANDSCAPE



TABLE OF CONTENTS

FOREWORD	5	2.3.6 Statement 6/2024 on the Second Report on the Application of the General Data Protection Regulation - Fostering Cross Regulatory Consistency and Cooperation	26
HIGHLIGHTS	7		
1. THE EDPB SECRETARIAT	10	2.4 STAKEHOLDER CONSULTATION	26
1.1 MISSION AND ACTIVITIES	11	2.4.1 Public Consultation on Guidelines	26
2. EUROPEAN DATA PROTECTION BOARD - ACTIVITIES IN 2024	15	2.4.2 Stakeholder Events	27
2.1 CONSISTENCY OPINIONS	17	2.4.3 Survey on Practical Application of Adopted Guidance	27
2.1.1 Art. 64(1) GDPR Opinions	17		
2.1.2 Art. 64(2) GDPR Opinions	18		
2.2 GENERAL GUIDANCE	23	2.5 REPRESENTING THE EDPB WORLDWIDE	28
2.2.1 Guidelines 01/2023 on Article 37 of the Law Enforcement Directive (LED)	23	3. ENFORCEMENT COOPERATION AND ENFORCEMENT BY DPAS	30
2.2.2 Guidelines 02/2023 on the Technical Scope of Art. 5(3) of the ePrivacy Directive	24	3.1 EDPB ACTIVITIES TO SUPPORT GDPR ENFORCEMENT AND COOPERATION AMONG DPAS	30
2.2.3 Guidelines 01/2024 on processing of personal data based on Article 6(1)(f) GDPR	24	3.2 COOPERATION UNDER THE GDPR	32
2.2.4 Guidelines 02/2024 on Article 48 GDPR	24	3.3 BINDING DECISIONS	34
2.3 STATEMENTS ON LEGISLATIVE DEVELOPMENTS	24	3.4 CASE DIGEST	35
2.3.1 Statement 1/2024 on legislative developments regarding the Proposal for a Regulation laying down rules to prevent and combat child sexual abuse	24	3.5 NATIONAL CASES WITH EXERCISE OF CORRECTIVE POWERS	37
2.3.2 Statement 2/2024 on the financial data access and payments package	25	3.6 SELECTION OF NATIONAL CASES	39
2.3.3 Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework	25	3.6.1 AUSTRIA	39
2.3.4 Statement 4/2024 on the recent legislative developments on the Draft Regulation laying down additional procedural rules for the enforcement of the GDPR	25	3.6.2 BELGIUM	39
2.3.5 Statement 5/2024 on the Recommendations of the High-Level Group on Access to Data for effective Law enforcement	26	3.6.3 BULGARIA	40
		3.6.4 CROATIA	40
		3.6.5 CYPRUS	40
		3.6.6 CZECH REPUBLIC	41
		3.6.7 DENMARK	41
		3.6.8 ESTONIA	42
		3.6.9 FINLAND	42
		3.6.10 FRANCE	42
		3.6.11 GERMANY	43
		3.6.12 GREECE	43
		3.6.13 HUNGARY	44

EDPB Annual Report 2024

3.6.14	ICELAND	44
3.6.15	ITALY	45
3.6.16	IRELAND	45
3.6.17	LATVIA	46
3.6.18	LIECHTENSTEIN	47
3.6.19	LITHUANIA	47
3.6.20	LUXEMBOURG	47
3.6.21	MALTA	48
3.6.22	NETHERLANDS	48
3.6.23	NORWAY	49
3.6.24	POLAND	49
3.6.25	PORTUGAL	49
3.6.26	ROMANIA	50
3.6.27	SLOVENIA	51
3.6.28	SPAIN	51
3.6.29	SWEDEN	52
4.	ANNEXES	53
4.1	GENERAL GUIDANCE ADOPTED IN 2024	53
4.2	CONSISTENCY OPINIONS ADOPTED IN 2024	53
4.2.1	Art. 64(1) GDPR Opinions	53
4.2.2	Art. 64(2) GDPR Opinions	54
4.3	STATEMENTS ON LEGISLATIVE DEVELOPMENTS	54
4.4	OTHER DOCUMENTS	54



FOREWORD

It is with great pleasure that I present the European Data Protection Board's (EDPB) 2024 annual report. Reading this report, you will learn about the milestones the EDPB achieved in 2024, a year during which the Board has shown, once more, its commitment to upholding the fundamental right of privacy and data protection.

In April 2024, we adopted our new [strategy 2024-2027](#). The strategy outlines key priorities and actions to strengthen data protection, ensure consistent enforcement of the GDPR, and address emerging challenges in a rapidly evolving digital landscape. It will help us further strengthen, modernise and harmonise data protection across Europe via four main pillars and a series of key actions.

In 2024, we have also continued to provide guidance and legal advice. Remarkably, we did not issue any Art. 65 binding decisions in the past year, whilst we have observed a sharp increase in the number of requests for opinion on questions of general application, under Art. 64(2). For example, we adopted an [opinion on the validity of 'Consent or Pay' models deployed by large online platforms](#). The models we have today usually require individuals to either give away their data or to pay. As a result, most users consent to the processing in order to use a service, and they do not understand the full implications of their choices. According to our opinion, large online platforms will, in most cases, not be able to comply with the requirements for valid consent if they confront users only with a choice between consenting to processing of personal data for behavioural advertising purposes and paying a fee.

Art. 64(2) opinions are an important tool allowing for consistency from an early stage and several more of these opinions were adopted in 2024, including on the [notion of main establishment](#), the [use facial recognition at airports](#), the [reliance on processors and sub-processors](#), and [the use of personal data to train AI models](#).

With this last opinion, the EDPB aims to support responsible AI innovation by ensuring personal data used to train AI models are protected and in full respect of the General Data Protection Regulation (GDPR).

AI technologies may bring many opportunities and benefits to different industries and areas of life, and we need to ensure these innovations are done ethically, safely, and in a way that benefits everyone. In our opinion, we confirm AI developers can use legitimate interest as a legal basis for model training, under certain conditions. To help developers determine if they are using it lawfully, the EDPB put forward a three-step test.

New digital legislations, including the Digital Markets Act (DMA), the Digital Services Act (DSA), the AI Act, the Governance Act and the Data Act, have come into force recently. These legislations address a variety of important issues, and all of them are built on the foundation laid by the GDPR. Increasingly, we will find that fairness, contestability, and the protection of fundamental rights will need to be approached from multiple regulatory angles. This requires seamless cross-regulatory collaboration and the EDPB will actively contribute to it.

As we move into this new phase, the number of formal regulatory roles of the EDPB and Data Protection Authorities (DPAs) are expanding. On top of that, the EDPB already pro-actively seeks the input of other regulators. For example, the EDPB met with the EU AI Office and took on board its views prior to adopting the [opinion on AI Models](#).

Finally, the EDPB continued its efforts to provide information on the GDPR to a broad audience, presenting it in clear, non-technical language. To this end, our [Data Protection Guide for Small Business](#), previously launched in 2023, was made available in 18 languages in 2024. In addition, we launched a series of summaries of EDPB guidelines to help non-expert individuals and organisations identify in an easier way the most important points to consider.

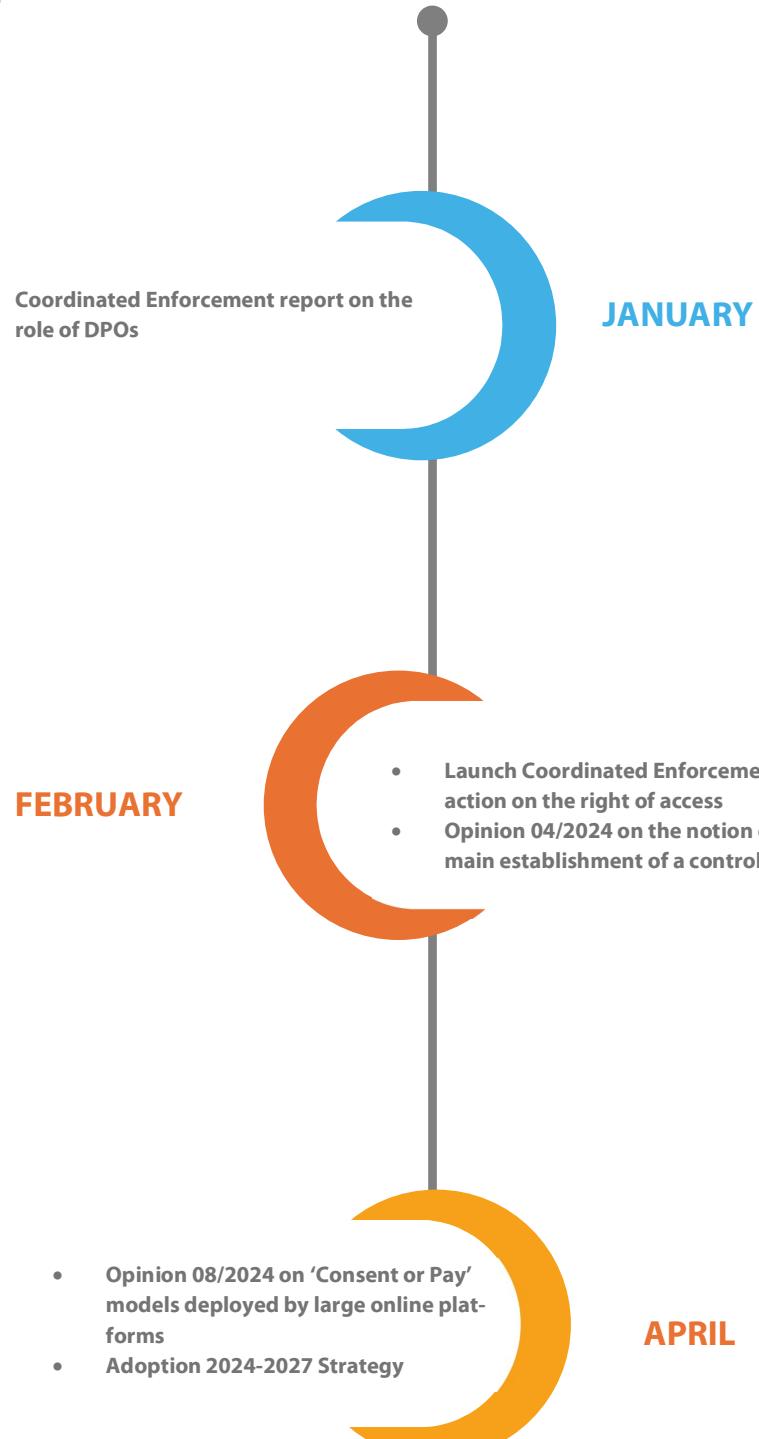
Chairing the EDPB over the last two years has been a true privilege, and I am confident that the work of the DPAs and the EDPB Secretariat will continue to strengthen data protection and privacy in the years to come.

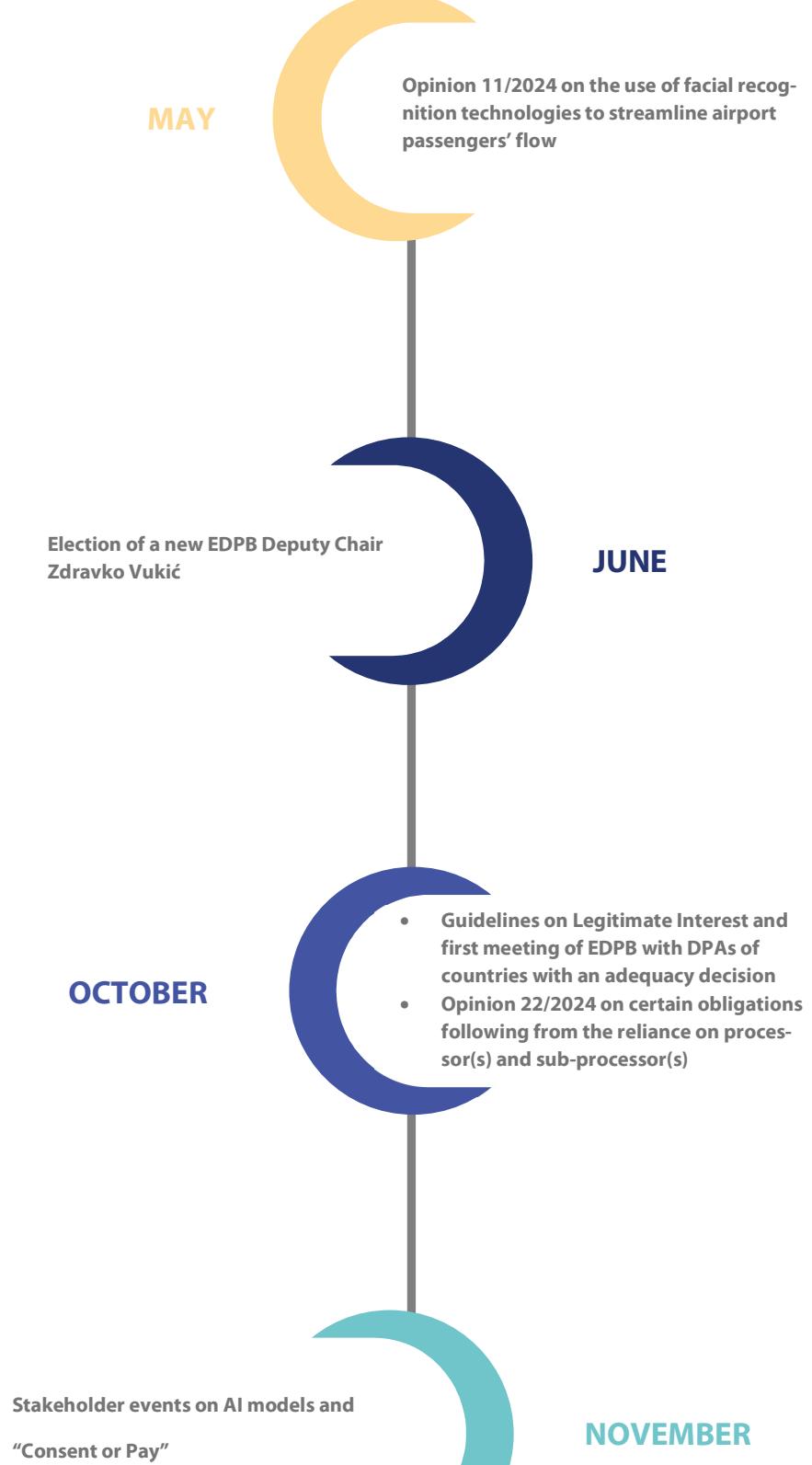
Anu Talus

Chair of the European Data Protection Board

HIGHLIGHTS

2024





DECEMBER



Opinion 28/2024 on AI models



1. THE EDPB SECRETARIAT

Reflecting on the work accomplished in 2024, we observe that the number of responsibilities of the EDPB has increased and that this has an impact on the work done by the EDPB Secretariat.

As we transitioned into a new regulatory digital framework¹, the EDPB proved ready to take on new roles, for example by becoming a member of the DMA High-Level Group, of the European Data Innovation Board (EDIB) or by cooperating with the European Board for Digital Services (EBDS). In 2024, the EDPB also cooperated with competition and consumer authorities and the AI office. This cross-regulatory cooperation as well as the launch of the work on several guidelines on the interplay between the GDPR and other digital regulations are part of the new [EDPB Strategy 2024-2027](#).

While it is the first year since 2020 that the EDPB did not adopt any binding decision, we saw an important increase of request for consistency opinions under Art. 64(2) GDPR.

These opinions deal with a matter of general application or producing effects in more than one Member State and have proven to be a crucial tool for the consistent application of the GDPR by Data Protection Authorities (DPAs) in the context of new technologies.

In 2024, the EDPB Secretariat organised two stakeholder events on topics having an important societal relevance, such as the use of personal data to train AI models and “Consent or Pay” mechanisms used for behavioural advertising. We hosted these events not only because we are committed to transparency, but also because we consider stakeholders’ input essential for the quality of our work.

In order to ensure that our guidance is accessible for non-experts, individuals (including children), and SMEs, we started to develop information sheets to share guidelines’ core messages.

¹ New digital legislations, including the Digital Markets Act (DMA), the Digital Services Act (DSA), the AI Act, the Governance Act and the Data Act.

This is a new activity in the same spirit as the [Data Protection Guide for Small Business](#) that we developed in 2023.

Another area of growth in 2024 was the support the EDPB Secretariat offers to the Coordinated Supervisory Committee (CSC), which ensures coordinated supervision of large scale IT systems and EU bodies and agencies. In 2024, the activity of the CSC was extended to the supervision of the Visa Information System (VIS), in addition to the Schengen Information System (SIS), Europol, the EPPO, Eurojust and IMI that were already falling under the framework of the EDPB activities. Substantial work has been dedicated to the preparation of the supervision of ETIAS. In the near future, the interoperability will interconnect seven EU-information systems, three existing systems (SIS, VIS, Eurodac and PrümII) and three new systems, yet to be set up (EES, ETIAS and ECRIS-TCN).

The increased activities of the Board led to a significant surge in the support the EDPB Secretariat offers to EDPB members. As figures sometimes speak louder than words, I believe it is important to mention that the EDPB Secretariat organised over 530 meetings in 2024 (up from over 360 in 2023) and managed over 4.200 requests for IT assistance and queries from our members (up from 3.400 in 2023).

To ensure that the EDPB Secretariat can continue to successfully perform its tasks and accomplish its mission, it is essential to get the appropriate resources in terms of staff and budget.

I would like to thank the EDPB Secretariat's staff and the Board's members who contributed to each single achievement we reached throughout 2024. This is a testament to the dedication of each of us, our steady cooperation and our commitment to ensuring the EDPB's daily operations run smoothly and effectively.

The work of the Secretariat will continue to evolve to meet the changing needs of the evolving technological and regulatory landscape, and together we stay strong in our commitment to further uphold the right of data protection across Europe and beyond in the years ahead.

Isabelle Vereecken

Head of the EDPB Secretariat



1.1 MISSION AND ACTIVITIES

The European Data Protection Board (EDPB) Secretariat offers analytical, administrative and logistical support to the Board. Its overarching mission is to ensure that the EDPB functions effectively, facilitating the adoption of binding decisions, legal opinions, consistency opinions and guidance under the [General Data Protection Regulation](#) (GDPR). Beyond its core legal work, the Secretariat acts as a vital communication channel, ensuring a cohesive and consistent approach to data protection across Europe.

The EDPB Secretariat assists the EDPB Members in enforcing data protection laws by fostering consistency and promoting cooperation among Data Protection Authorities (DPAs). For a limited number of complex cases where DPAs cannot reach a consensus, the EDPB issues binding decisions. As a neutral party among DPAs, the Secretariat provides essential support in drafting these decisions, ensuring impartiality and adherence to regulatory standards.

In 2024, the Secretariat's work reflected the growing complexity and breadth of the GDPR implementation. The Secretariat was instrumental in drafting eight consistency opinions under [Art. 64\(2\) GDPR](#), which provide guidance to national DPAs on any matter of general application or producing effects in more than one Member State. Any DPA, the Chair of the Board, or the European Commission may request such opinions, particularly in cases where a competent national authority is deemed not to fulfil its obligations regarding mutual assistance. These opinions provided authoritative guidance on cross-border data protection measures, addressing challenges unique to a rapidly evolving digital landscape. For instance, one consistency opinion focused on the processing of facial recognition to streamline airport passengers' flow, a subject of increasing importance as digital authentication methods evolve.

Furthermore, the Secretariat oversaw significant litigation activities, representing the EDPB as a party in multiple cases before the Court of Justice of the European Union (CJEU).

In 2024, the EDPB was involved as a main party in 13 cases before the CJEU, one of which was submitted in 2022,² ten in 2023,³ and two in 2024.⁴ Most of the cases concerned applications for annulment against binding decisions adopted by the EDPB. The two cases submitted in 2024 concerned applications for annulment against an urgent binding decision and against an opinion. In addition, in 2024 the EDPB was involved as intervener in one case, in support of the European Data Protection Supervisor (EDPS). During all these proceedings, the Secretariat of the EDPB collaborated closely with external lawyers at every stage. This included defining the EDPB's legal strategy, drafting procedural documents, and preparing for and attending hearings before the CJEU.



"The EDPB is a dynamic and collaborative body that plays a pivotal role in ensuring the consistent application of data protection laws across Europe. From my perspective as Deputy Chair, I see it as a guardian of individuals' privacy rights, skilfully balancing the needs of innovation and economic growth. Our diverse membership strengthens our ability to address complex data protection issues and fosters a culture of shared responsibility among member states."

Zdravko Vukić
Director of the Croatian Personal Data Protection Agency and EDPB Deputy Chair

In addition, the EDPB Secretariat provides the Secretariat of the [Coordinated Supervision Committee](#) (CSC). The CSC ensures the coordinated supervision of large-scale IT systems and of European Union bodies, offices and agencies, in accordance with Art.62 of [Regulation \(EU\) 2018/1725](#) or with the EU legal act establishing the large scale IT system or the EU body, office or agency.

Budget management remained a priority in 2024. The EDPB budget forms part of the broader budget of the EDPS. Operating within an approved budget of €8.36 million, the Secretariat effectively allocated resources to support enforcement, litigation, and operational activities.

Operational structure

The EDPB Secretariat has evolved into a robust and dynamic organisation. It comprises a team of 39⁵ highly specialised professionals dedicated to supporting the Board's activities. Organised into five distinct sectors focusing on legal affairs, litigation and international affairs, IT matters, information and communications, and administrative matters, the Secretariat ensures that all aspects of the EDPB's mandate are addressed comprehensively.

While formally employed by the EDPS, the Secretariat staff operate under the exclusive direction of the EDPB Chair. The cooperation framework between the EDPB and the EDPS is defined by a [Memorandum of Understanding](#). This structure facilitates seamless collaboration and ensures that the Secretariat can fully dedicate its resources to supporting the Board's work. In 2024, the Secretariat prioritised staff development, introducing targeted training programs on emerging technologies such as AI to better address future challenges in data protection.

² Case T-682/22 Meta Platforms Ireland v EDPB.

³ Cases T-183/23 Ballmann v European Data Protection Board; Joined cases T-70/23, T-84/23, 111/23 Data Protection Commission v European Data Protection Board; T-128/23 Meta Platforms Ireland v European Data Protection Board; T-129/23 Meta Platforms Ireland v European Data Protection Board; T-153/23 WhatsApp Ireland v EDPB; T-325/23 Meta Platforms Ireland v European Data Protection Board; T-1030/23 Tiktok Technology v

European Data Protection Board and C-97/23 P WhatsApp Ireland v EDPB.

⁴ Case T-8/24 Meta Platforms Ireland v EDPB and Case T-319/24 Meta Platforms Ireland v EDPB.

⁵ The EDPB budget covers 46 posts, including seven posts at the EDPS for the support provided to the EDPB via horizontal administrative services.

Data protection and transparency

The EDPB Secretariat is also responsible for handling Access to Documents (AtD) requests, in accordance with Art. 32(2) of the EDPB Rules of Procedure (RoP). These activities ensure transparency and accountability in the Board's operations by facilitating public access to the EDPB documents.

Initial AtD requests are handled and signed by one of the Deputy Chairs. Confirmatory requests are handled and signed by the Chair. In 2024, the EDPB received 38 access requests for documents held by the EDPB. Confirmatory applications were received in three cases. No complaint regarding the EDPB confirmatory decisions for a request for access to documents was brought to the attention of the European Ombudsman in 2024.

The EDPB processes personal data according to the rules laid down in Regulation (EU) 2018/1725 on the processing of personal data by the Union institutions, bodies, offices and agencies. In accordance with Art. 43 of this Regulation, the EDPB has its own Data Protection Officer (DPO) team, which is part of the EDPB Secretariat. In 2024, the EDPB received 18 individual requests based on rights enshrined in Art. 17 to Art. 24 of Regulation (EU) 2018/1725. The EDPB Secretariat also provided assistance with replying to individual requests for information involving the processing of their personal data and supported in handling six data breaches under Arts. 34 and 35 of Regulation (EU) 2018/1725, one of which required a notification to the EDPS.

IT systems

In 2024, the EDPB Secretariat achieved significant advancements in its IT systems, continuing to enhance cooperation and communication among DPAs. The Internal Market Information (IMI) system remained a fundamental part of the GDPR cooperation, facilitating over 5.644 procedures during the

The Secretariat handled 907 support requests related to the IMI system and managed a total of 4.225 inquiries across all the EDPB IT systems, ensuring timely and effective assistance for all stakeholders.

In addition, the EDPB Secretariat introduced a centralised training resource to improve the accessibility and effectiveness of its IT tools. This hub offers detailed guidance on how information is structured within the primary EDPB information exchange platform and provides various user guide materials for using the various EDPB IT systems. Furthermore, the EDPB Secretariat developed a comprehensive series of videos showcasing the key features of these IT systems, further promoting efficient collaboration.

The EDPB HUB, the primary platform for internal communication and information sharing, experienced significant growth in 2024. Over 12.307 content pieces were created and shared, reflecting a substantial 64% increase compared to the previous year. This included 2.372 new pages, making a 59% rise, and 8.217 documents, which represents 72% growth. Exchanges also increased, reaching 1.389, a 37% more over 2023, alongside 329 other types of content. With a user base now exceeding 1.500 Members (a 7% increase) the platform continues to be a vital tool for collaboration and innovation.

The Secretariat also ensured the uninterrupted operation of the EDPB website, which received 329.432 visits over the course of the year. The most frequently accessed sections included Guidelines, Recommendations, Best Practices, Documents, Opinions, the Cookie Policy, Career opportunities, Binding Decisions, Contact us and News.

These digital platforms continue to play a critical role in advancing the EDPB's mission and enhancing its operational efficiency.

EDPB SECRETARIAT | ORGANISATIONAL CHART





2. EUROPEAN DATA PROTECTION BOARD – ACTIVITIES IN 2024



"The year 2024 has once again confirmed the importance of cooperation between European data protection authorities in responding to the concerns of individuals and, where necessary, punishing breaches of the regulations. Faced with the major technological and societal challenges of today, particularly those relating to artificial intelligence, cybersecurity and the rights of minors, it is more necessary than ever to strengthen our synergies and harmonise our practices."

Marie-Laure Denis
Head of French Data Protection Authority

2024-2027 Strategy and 2024-2025 Work Programme

In 2024, the EDPB remains steadfast in its mission to consistent application of data protection laws across Europe while fostering stronger collaboration among DPAs. The [2024-2027 Strategy](#) and the [2024-2025 Work Programme](#) provide a comprehensive roadmap to address emerging challenges, safeguard fundamental rights, and adapt to the rapid evolution of digital technologies.

Structured around four key pillars, the 2024-2027 Strategy guides the EDPB's actions and priorities:

- **Pillar 1 on advancing harmonisation and promoting compliance** aims at ensuring consistent and effective application of data protection laws across countries;
- **Pillar 2 on reinforcing a common enforcement culture** aims at strengthening collaboration among DPAs to address complex cases and enhance cross-border cooperation;
- **Pillar 3 on addressing technological challenges** aims at emphasising a human-centric approach to emerging technologies, safeguarding fundamental rights, and navigating an evolving regulatory landscape;

- **Pillar 4 on enhancing the EDPB's global role** aims at engaging with international partners to promote high data protection standards worldwide.

The 2024-2025 Work Programme is the first of two which will implement the EDPB Strategy for 2024–2027. It is based on the priorities set out in the EDPB Strategy.

The Work Programme lists several key actions, which serve to implement the EDPB Strategy. These include:

- Providing concise, practical and clear guidance that is accessible to the relevant audience, as well as tools and content for a non-expert audience, including particularly vulnerable data subjects such as children;
- Supporting the development of compliance measures and engagement with stakeholders;
- Strengthening efforts to ensure effective enforcement of the GDPR and cooperation between the Members of the EDPB, building on its commitments made in the Vienna Statement on enforcement cooperation and on the opportunities arising from the future Regulation on the GDPR procedural rules;
- Establishing common positions and guidance in the cross-regulatory landscape and cooperating with other regulatory authorities on matters relating to data protection, including competition authorities, consumer protection authorities and authorities competent under other legal acts;
- Monitoring and assessing new technologies;
- Promoting a global dialogue on privacy and data protection, including a focus on the international community, and supporting cooperation on enforcement between EU and non-EU authorities.

New roles and responsibilities in a changing environment

In response to the unprecedented pace of technological advancement, the EU implemented a series of digital laws in 2024. These regulations have expanded the responsibilities of DPAs, giving them new roles in overseeing compliance and safeguarding data protection.

The AI Act designates DPAs (or other authorities with the same requirements on independence) as Market Surveillance Authorities (MSA) for certain high-risk AI systems, reinforcing their central role in protecting data protection rights.

Similarly, under the Data Act, DPAs ensure personal data processing aligns with the GDPR standards, supported by enhanced cooperation frameworks to manage new regulatory demands.

As a Member of the High-Level Group on the Digital Markets Act (DMA), the EDPB provided critical guidance to the European Commission, fostering a cohesive and harmonised regulatory approach across data governance frameworks. This collaboration ensured alignment between data protection law and sectoral regulations, reflecting the interconnected nature of digital governance.

The EDPB also actively participated in the European Board for Digital Services, addressing critical issues within the internal market. Its efforts included supporting the oversight of large online platforms and search engines and contributing to the Age Verification Taskforce. As a Member of the European Data Innovation Board, the EDPB played a pivotal role in initiatives related to data sharing and the development of European data spaces. These responsibilities align with the Board's broader mission to address complex, cross-border and cross-regulatory challenges in the digital era.



"The European Data Protection Board (EDPB) drives global privacy standards by ensuring consistent GDPR application, fostering transparency and trust. In the world of new technologies, the EDPB will play a crucial role in guiding innovation while protecting privacy, strengthening international cooperation, and addressing emerging challenges in the digital environment."

Dijana Šinkūnienė
Director of the State Data Protection Inspectorate of the Republic of Lithuania



"Cooperation through EDPB is one of my priorities as the new Slovenian Information Commissioner. Data protection in the EU would undoubtedly be much weaker without the EDPB and GDPR. Especially with the challenges brought by the digital landscapes and the new duties the DPAs will be having in the AI regulatory framework."

**Dr. Jelena Virant Burnik
Information Commissioner of the
Republic of Slovenia**

2.1 CONSISTENCY OPINIONS

Consistency opinions are a driving force of the EDPB's mission to ensure the uniform interpretation and application of the GDPR across the EU. Established under Art. 64 GDPR, these opinions provide authoritative, non-binding recommendations that align DPAs decisions with a common EU framework. By addressing areas of potential divergence, consistency opinions contribute to harmonised enforcement and legal clarity.

DPAs may request a consistency opinion from the EDPB when considering measures that could impact multiple jurisdictions. Once issued, these opinions serve as guiding documents, enabling DPAs to finalise their decisions while ensuring alignment with the GDPR standards. In 2024, 28 opinions were issued under two distinct mechanisms: Art. 64(1) GDPR and Art. 64(2) GDPR, each addressing specific regulatory needs and challenges.

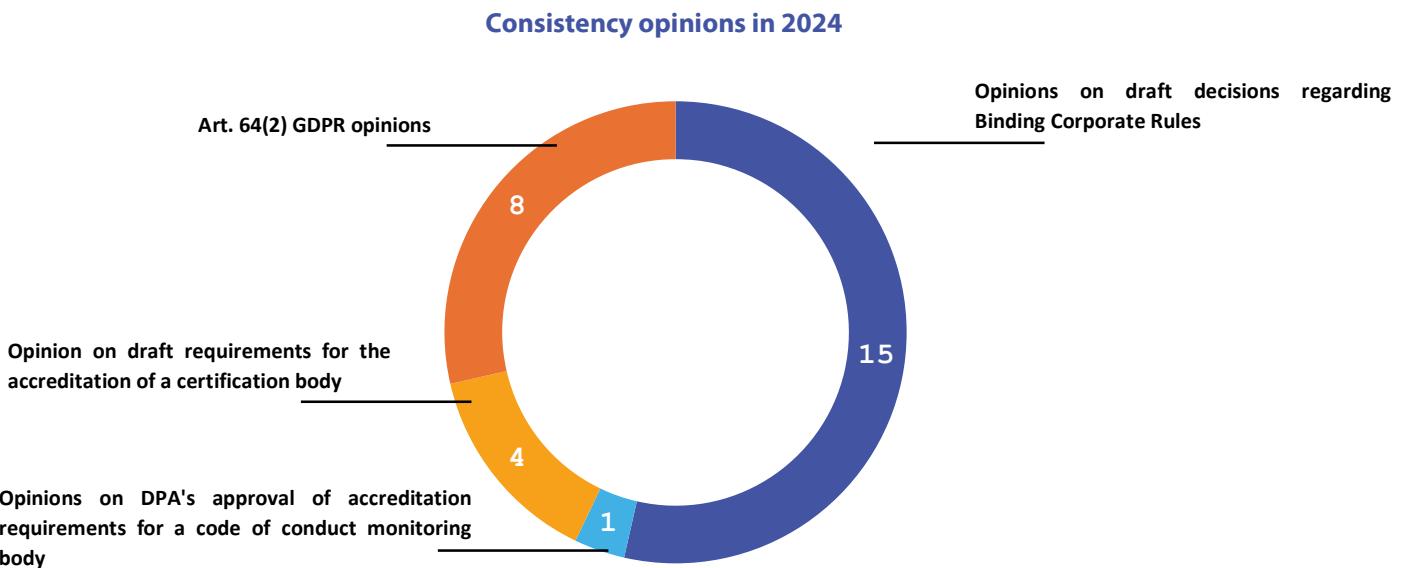
2.1.1 Art. 64(1) GDPR Opinions

Art. 64(1) GDPR mandates the issuance of consistency opinions for specific measures that DPAs intend to adopt. These opinions are pivotal in ensuring the uniform application of the GDPR provisions and fostering regulatory coherence across countries. The six categories of

measures requiring consistency opinions under Art. 64(1) GDPR include:

- Lists of processing operations requiring Data Protection Impact Assessments (DPIAs): these lists identify activities that are likely to pose significant risks to individuals' rights and freedoms;
- Draft codes of conduct: tailored to specific sectors or processing activities, these codes facilitate compliance by providing industry-specific guidance while ensuring alignment with the GDPR principles;
- Accreditation of certification bodies, of criteria for certification bodies, and schemes: these criteria establish the standards for certification, promoting trust and accountability in data protection;
- Draft decisions on standard contractual clauses (SCC) for international data transfers: these clauses provide legally robust mechanisms for transferring personal data outside the EU, ensuring continuity in data protection;
- Authorisations for custom contractual clauses: bespoke clauses tailored to specific circumstances, requiring the EDPB review to ensure compliance with the GDPR requirements;
- Approvals of Binding Corporate Rules (BCRs): these rules govern intra-group data transfers within multinational organisations, ensuring consistent application of the GDPR principles across jurisdictions.

In 2024, the EDPB adopted 20 Art. 64(1) GDPR opinions, reflecting its continued commitment to promoting harmonisation. Since its establishment in 2018, the EDPB has issued a total of 188 Art. 64(1) opinions, demonstrating the sustained importance of this mechanism in supporting a harmonised application of the GDPR. **See Section 4.2.1 for the complete list of opinions adopted in 2024.**



2.1.2 Art. 64(2) GDPR Opinions

Art. 64(2) GDPR provides a mechanism for the EDPB to issue consistency opinions on matters of general application or those with significant cross-border implications. Such opinions can be requested by the EDPB Chair, DPAs, or the European Commission to address broad, recurring issues or complex legal questions, ensuring alignment across Member States. These opinions help avoid conflicting DPAs decisions and ensure that the GDPR rules are applied consistently in the EU.

In 2024, the EDPB adopted eight Art. 64(2) GDPR opinions, highlighting the growing importance of this mechanism in addressing critical data protection challenges. **See Section 4.2.2 for the complete list of opinions adopted in 2024.**

2.1.2.1 Opinion 4/2024 on the notion of main establishment of a controller in the Union under Article 4(16)(a) GDPR

In February 2024, the EDPB issued [Opinion 4/2024](#) following a request by the French DPA to clarify the notion of "main establishment" of a data controller in the Union pursuant to Art. 4(16)(a) GDPR.

Scope of the Opinion

The notion of "main establishment" is pivotal in determining the lead DPA responsible for overseeing a data controller's compliance with the GDPR and has therefore important consequences for the practical application of the one-stop-shop mechanism.

In its request to the Board, the French DPA asked whether:

- For a data controller's "place of central administration in the Union" to be qualified as a main establishment under Art. 4(16)(a) GDPR, this establishment should take decisions on the purposes and means of the processing and have the power to have them implemented;
- The one-stop-shop mechanism applies only if there is evidence that one of the establishments in the Union of the data controller (the data controller's "place of central administration" or not) takes the decisions on the purposes and means concerning the processing operations in question and has the power to have such decisions implemented.

Key considerations

Based on Art. 4(16)(a) GDPR, the EDPB determined that a "place of central administration" in the EU should be considered the main establishment only if it makes decisions regarding the purposes and means of personal data processing and has the authority to implement those decisions.

The EDPB further explained that the one-stop-shop mechanism can only apply if there is evidence that one of the establishments of the data controller in the Union takes decisions on the purposes and means for the relevant processing operations and has the power to have these decisions implemented. This means that, when the

decisions on the purposes and means of the processing are taken outside of the EU, there should be no main establishment of the data controller in the Union, and therefore the one-stop-shop should not apply.

Practical implications and recommendations

The EDPB provided useful clarifications on how the DPAs should apply in practice Art. 4(16)(a) GDPR to ensure its uniform application. In particular, the EDPB recalled that the burden of proof in relation to the place where the relevant processing decisions are taken and where there is the power to implement such decisions in the Union ultimately falls on data controllers.

In addition, the DPAs retain the ability to challenge the data controller's claim based on an objective examination of the relevant facts, requesting further information where required. The EDPB further stated that when determining the location of the data controller's main establishment, DPAs should duly cooperate and jointly agree, depending on the concrete case, on the level of detail the data controller should provide.

2.1.2.2 **Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms**

In April 2024, the EDPB adopted [Opinion 08/2024](#) on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, following a request from the Dutch, Norwegian, and German (Hamburg) DPAs. This Opinion addresses whether consent, as defined under Art. 4 (11) GDPR, is valid and, in particular, "freely given", when users face a stark choice between allowing data processing for behavioural advertising or paying a fee for an alternative service.

Acknowledging the cross-regulatory implications, the EDPB collaborated with national and EU-level competition and consumer protection regulators to integrate broader perspectives into its assessment. This cooperation has proven very useful in providing valuable input for the Opinion on Consent or Pay.

Scope of the Opinion

The scope of this Opinion is limited to the use of "Consent or Pay" models by large online platforms, defined by their significant reach and influence over millions of users across the EU. These platforms often leverage behavioural advertising as a primary revenue stream, offering services where users are asked either to consent to the processing of their personal data for advertising purposes or to pay a fee to access an ad-free or data-minimised version of the service. The Opinion draws on the GDPR and relevant case law, particularly the July 2023 ruling by the Court of Justice

of the European Union (CJEU) in the Bundeskartellamt case (C-252/21), which addressed issues of consent and power imbalance in the context of large online platforms.

Key considerations

The EDPB reiterated several core principles of the GDPR in its assessment, particularly:

- **Necessity and proportionality:** processing personal data for behavioural advertising must be proportionate to the purpose and limited to what is strictly necessary. The "Consent or Pay" models, as commonly implemented, often fail to meet these standards;
- **Fairness and accountability:** data controllers must ensure that users fully understand the implications of consenting to data processing. The Board emphasised the importance of fairness in offering a real choice without undue pressure or coercion. Data controllers must also document how consent is obtained and ensure they can demonstrate compliance with the GDPR's accountability principle;
- **Granularity and transparency:** consent must be specific and granular. Users should be able to consent to purposes for data processing without being forced into a bundled consent covering multiple, distinct purposes. Platforms must clearly explain each option and its implications in accessible and plain language;
- **Conditionality:** consent is presumed not to be freely given if it is conditional on accessing a service where processing is not necessary for the provision of that service. Platforms that offer only two stark choices – consenting to intrusive behavioural advertising or paying a fee – may fail to provide a true alternative and may undermine the principle of free consent.

The challenges of "Consent or Pay" models

The Board recognised that "Consent or Pay" models by large online platforms often do not satisfy the GDPR's requirement that consent must be freely given. Many users feel pressured to consent to data processing rather than pay, particularly when services are part of individuals' daily lives, or essential to social interactions, or professional networking. The Opinion further elaborates on the risks of these models, identifying three primary issues:

- **Imbalance of power:** in many cases, large online platforms hold a dominant market position, limiting users' ability to reject consent without significant detriment. The CJEU Bundeskartellamt case underlined that a platform's dominant position could hinder users from refusing consent, as their ability to choose an alternative service is often limited or non-existent;
- **Detriment to users:** the EDPB stressed that consent cannot be considered freely given if the user suffers detriment for refusing. For instance, if users are excluded from accessing important services or social interactions due to non-consent, this would undermine the validity of their choice. The financial burden of paying for an ad-free version can also be seen as a detriment, particularly when the fee is prohibitively high;
- **Lack of genuine alternatives:** to provide a real choice, the EDPB emphasised the importance of offering an "equivalent alternative" that does not require either payment or extensive personal data collection. For example, platforms could offer a version with non-personalised advertising, where only minimal and non-behavioural data is collected. Providing this type of alternative helps mitigate concerns about the validity of consent.

Recommendations for DPAs

The EDPB made considerations for DPAs to take into account when large online platforms seek to comply with the GDPR when implementing "Consent or Pay" models:

- **Offer a free alternative without behavioural advertising:** platforms should consider providing a version of their service that does not rely on behavioural advertising but instead uses less intrusive forms of advertising, such as contextual ads based on the content viewed. This would allow users to enjoy the service without the need to consent to invasive data processing or pay a fee. DPAs should also consider more generally if consent is freely given, if there is an imbalance of power and if the individual would suffer detriment as a consequence of not consenting. Consent should also be specific;
- **Transparency and information:** users must be fully informed about the consequences of their choices. The EDPB considers that platforms should adopt clear and simple communication to ensure users understand what data is collected, how it is used, and what opting out or paying entails;

- **Avoiding high fees:** any fee charged for accessing a service without behavioural advertising should be proportionate and must not discourage users from exercising their right to refuse consent. Excessive fees that compel users to consent instead of paying for the alternative are not acceptable under the GDPR.

The EDPB concluded that most current implementations of "Consent or Pay" models by large online platforms are unlikely to meet the GDPR's strict requirements for valid consent. To this end, the EDPB will also be developing further guidelines on the use of 'Consent or Pay' models, with a broader scope and stakeholder engagement.

This Opinion marks a significant step in addressing the growing concerns over the use of personal data by large online platforms and the ways in which users' consent is obtained. The EDPB remains committed to ensuring that the fundamental right to data protection is upheld, especially in the face of increasingly complex business models that seek to monetise personal data.

2.1.2.3 [Opinion 11/2024 on the use of facial recognition to streamline airport passengers' flow](#)

In May 2024, the EDPB issued [Opinion 11/2024](#) on the use of facial recognition technologies by airports and airlines to streamline passengers' flow.

Scope of the opinion

The French DPA requested this Opinion due to increasing deployment of biometric systems at major airports across the EU, raising significant data protection concerns. The EDPB's role was to ensure that such systems comply with the GDPR principles while safeguarding individuals' fundamental rights to privacy and data protection.

Key considerations

Facial recognition technologies are often promoted as tools to enhance efficiency and convenience in the travel industry. However, these systems also involve the processing of sensitive biometric data, necessitating compliance with Art. 5(1)(e) GDPR, Art. 5(1)(f) GDPR, Art. 25 GDPR, and Art. 32 GDPR, among others.

There is no uniform legal requirement in the EU for airport operators and airline companies to verify that the name on the passenger's boarding pass matches the name on their identity document, and this may be subject to national laws. Therefore, where no verification of the passengers' identity with an official identity document is required, no such verification with the use of biometrics should be performed, as this would result in an excessive processing of data.

Different storage solutions and their implications

In its Opinion, the EDPB considered the compliance of processing of passengers' biometric data with four different types of storage solutions, ranging from ones that store the biometric data only in the hands of the individual to those which rely on a centralised storage architecture with different modalities. In all cases, only the biometric data of passengers who actively enrol and consent to participate should be processed.

The EDPB found that the only storage solutions which could be compatible with the integrity and confidentiality principle, data protection by design and default and security of processing, are the solutions whereby the biometric data is stored in the hands of the individual or in a central database but with the encryption key solely in their hands. These storage solutions, if implemented with a list of recommended minimum safeguards, are the only modalities which adequately counterbalance the intrusiveness of the processing by offering individuals the greatest control. The EDPB found that the solutions that were examined and which are based on the storage in a centralised database either within the airport or in the cloud, without the encryption keys in the hands of the individual, cannot be compatible with the requirements of data protection by design and default and, if the data controller limits themselves to the measures described in the scenarios analysed, would not comply with the requirements of security of processing.

2.1.2.4 [Opinion 22/2024 on certain obligations following from the reliance on processor\(s\) and sub-processor\(s\)](#)

In October 2024, the EDPB adopted [Opinion 22/2024](#) concerning certain obligations of data controllers when engaging data processors and sub-processors, stemming from the requirements of Art. 28 GDPR and in light of the principle of accountability. This Opinion was requested by the Danish DPA.

Scope of the Opinion

The Opinion is about situations where controllers rely on one or more processors and sub-processors. In particular, it addresses questions on the interpretation of certain duties of controllers in such a situation, as well as the wording of controller-processor contracts. The questions address processing of personal data in the European Economic Area (EEA) as well as processing following a transfer to a third country.

Key considerations

The Opinion explains that controllers should have the information on the identity (i.e. name, address, contact person) of all processors, sub-processors etc. readily available

at all times so that they can best fulfil their obligations under Art. 28 GDPR.

Art. 28(1) GDPR provides that controllers have the obligation to engage processors providing 'sufficient guarantees' to implement 'appropriate' measures in such a manner that the processing will meet the requirements of the GDPR and ensure the protection of the rights of individuals. In its Opinion, the EDPB considers that this verification obligation should apply regardless of the risk to the rights and freedoms of individuals. However, the extent of such verification may vary, notably based on the risks associated with the processing.

The Opinion also states that while the initial processor should ensure that it proposes sub-processors with sufficient guarantees, the ultimate decision and responsibility on engaging a specific sub-processor remains with the controller. DPAs should assess whether the controller is able to demonstrate that the verification of the sufficiency of the guarantees has taken place to the controller's satisfaction. The controller may choose to rely on the information received from its processor and build on it if needed. More specifically, for processing presenting a high risk to the rights and freedoms of individuals, the controller should increase its level of verification in terms of checking the information provided. In that regard, the EDPB considers in the Opinion that the controller does not have a duty to systematically ask for the sub-processing contracts to check if data protection obligations have been passed down the processing chain. The controller should assess whether requesting a copy of such contracts or reviewing them is necessary for it to be able to demonstrate compliance with the GDPR.

Transfers outside the EEA

In addition, where transfers of personal data outside of the EEA take place between two (sub-) processors, the data processor as data exporter should prepare the relevant documentation, such as relating to the ground of transfer used, the transfer impact assessment and possible supplementary measures. However, the data controller should assess this documentation and be able to show it to the competent DPA.

Data controller- data processor contracts

The EDPB also addresses, in the Opinion, a question on the wording of controller-processor contracts. In this respect, a basic element is the commitment for the processor to process personal data only on documented instructions from the controller, unless the processor is "required to [process] by Union or Member State law to which the processor is subject" (Art. 28(3)(a) GDPR). In light of the contractual freedom afforded to the parties within the limits of Art. 28(3) GDPR, the EDPB takes the view that including the terms quoted above (either verbatim or in

very similar terms) is highly recommended but not mandatory. As to variants similar to “unless required to do so by law or binding order of a governmental body” the EDPB takes the view that this remains within the contractual freedom of the parties and does not infringe Art. 28(3)(a) GDPR per se. At the same time, the EDPB identifies a number of issues in its Opinion, as such a clause does not exonerate the processor from complying with its obligations under the GDPR. For personal data transferred outside of the EEA, the EDPB considers it unlikely that this variant, in itself, suffice to achieve compliance with Art. 28(3)(a) GDPR in conjunction with Chapter V. Art. 28(3)(a) GDPR does not prevent - in principle - the inclusion in the contract of provisions that address third country law requirements to process transferred personal data. However, a distinction should be made between the third country law(s) which would undermine the level of protection guaranteed by the GDPR and those that would not.

This Opinion contributes to a harmonised interpretation by the DPAs of certain aspects of Art. 28 GDPR, where appropriate, in conjunction with Chapter V GDPR on transfers.



"We would like to express our deep appreciation and gratitude to our European Data Protection Board colleagues, and Secretariat, for guiding the EDPB through the Article 64.2 AI Opinion file, which concluded fittingly at the EDPB's 100th meeting.

Through this intensive process we have collectively secured an important step towards harmonisation at a European level on some of the key issues. This opinion addresses key questions of systemic importance on how responsible AI innovation can be supported by ensuring personal data are protected under the GDPR."

**Dr. Des Hogan
Commissioner (Chairperson)
for Data Protection, Ireland**

**Dale Sunderland
Commissioner for Data Protection,
Ireland**

2.1.2.5 **Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models**

On 18 December 2024, the EDPB adopted [Opinion 28/2024](#), addressing critical data protection questions surrounding the use of personal data in the development and deployment of Artificial Intelligence (AI) models.

Scope of the Opinion

The Opinion responds to a request from the Irish DPA under Art. 64(2) of the GDPR, with a focus on harmonising regulatory guidance in key areas. It examines the conditions under which an AI model trained on personal data can be considered anonymous. It also evaluates the use of legitimate interest as a legal basis for data processing in the development and deployment of AI models, considering the balance between innovation and individuals' rights.

Furthermore, it assesses the implications of unlawful data processing during an AI model's development and the extent to which such processing affects its subsequent use. While recognising the transformative potential of AI, the Opinion underlines the necessity of aligning technological advancement with the principles of the GDPR, including accountability, transparency, data minimisation, and the right to data protection.

Key considerations

1. Anonymity of AI Models

The Opinion highlights that AI models trained on personal data cannot always be considered anonymous. Claims of anonymity require a case-by-case assessment by DPAs. To establish anonymity, it must be improbable that personal data can be directly extracted or obtained through queries from the model, considering all reasonably likely means of identification. To conduct their assessment, DPAs should review the documentation provided by the controller to demonstrate the anonymity of the model. In that regard, the Opinion provides a non-prescriptive and non-exhaustive list of methods that may be used by controllers in their demonstration of anonymity and thus be considered by DPAs when assessing a controller's claim of anonymity.

2. Legitimate interest as a legal basis

The EDPB emphasises that there is no hierarchy between the legal bases. The Opinion then recalls the three-step test that should be conducted when assessing the use of legitimate interest as a legal basis, i.e. (1) identifying the legitimate interest pursued by the controller or a third party; (2) analysing the necessity of the processing for the

purposes of the legitimate interest(s) pursued (also referred to as "necessity test"); and (3) assessing that the legitimate interest(s) is (are) not overridden by the interests or fundamental rights and freedoms of the data subjects (also referred to as "balancing test"). The Opinion provides practical examples, such as developing AI for fraud detection or cybersecurity, where legitimate interest could apply, provided that strict safeguards are in place.

3. Impact of unlawful processing

Finally, when an AI model was developed with unlawfully processed personal data, this could have an impact on the lawfulness of its deployment, unless the model has been duly anonymised. Opinion 28/2024 reinforces the EDPB's commitment to ensuring that AI innovations respect GDPR principles while enabling responsible technological advancements. The Opinion sets the stage for continued guidance, including forthcoming guidelines on web scraping.



"DPAs' size is not important. Sometimes, even mouses can roar. Dealing with mega-organisations such as those handling adult-content websites, has proved quite a challenge in 2024, but we successfully completed our task. As Deputy Chair of the EDPB I have experienced first-hand the challenges it faces. Yet it is growing stronger. It has proved itself as a major key-player in the international data protection field. In coming years, it will continue improving its image and to provide guidance, where needed."

Irene Loizidou Nicolaïdou
Cypriot Commissioner for Personal Data Protection and EDPB Deputy Chair

2.2 GENERAL GUIDANCE

The EDPB plays a pivotal role in clarifying and harmonising the application of the GDPR through the issuance of comprehensive guidance.

Since entry into application of the GDPR, the EDPB has established a robust compendium of guidelines that address critical areas of data protection. These efforts have not only reinforced the consistency of enforcement among countries but have also strengthened compliance by offering practical solutions tailored to evolving technological and legal landscapes. The Board's guidelines are developed with a strong emphasis on stakeholder engagement, incorporating feedback gathered through public consultations to ensure they address real-world concerns effectively.

In 2024, the EDPB adopted four guidelines, two of which were finalised following public consultation initiated in 2023. See *Section 4.1* for the complete list of guidelines.

2.2.1 Guidelines 01/2023 on Article 37 of the Law Enforcement Directive (LED)

Adopted on 19 June 2024, these [Guidelines](#) address Art. 37 of the LED concerning cross-border data transfers by law enforcement authorities of EU countries. In particular, they explain the relevant factors to take into account when assessing whether the safeguards put in place for such transfers are "appropriate". The Guidelines build on the previous [Recommendations of the EDPB on the adequacy referential under the LED](#) and the [EDPB Statement on internal agreements including transfers](#).

Key recommendations outlined in the Guidelines include:

- **Appropriate safeguards:** they explain the essential requirements for appropriate safeguards to ensure an essentially equivalent level of data protection within the framework of Art. 37;
- **Expectations regarding legally binding instruments:** the EDPB identifies the elements that should, among other aspects, be addressed in such transfer tools (Art. 37(1)(a) LED);
- **Assessment of the transfer circumstances:** the Guidelines provide factors to take into account when competent authorities assess the risk surrounding transfers (Art. 37(1)(b) LED).

By offering this detailed guidance, the EDPB aims to support on the one hand, law enforcement authorities wishing to transfer personal data to third-country authorities or international organisations and, on the other hand, EU countries which negotiate legally binding instruments that serve as tools for such transfers.

2.2.2 Guidelines 02/2023 on the Technical Scope of Art. 5(3) of the ePrivacy Directive

Adopted on 7 October 2024, these [Guidelines](#) address the evolving challenges posed by modern online tracking technologies. Art. 5(3) of the ePrivacy Directive regulates the storage and access of information on users' terminal equipment, ensuring such activities are based on user consent or strict necessity.

The Guidelines clarify the scope of this provision, covering technologies such as:

- URL and pixel tracking;
- Local processing;
- Tracking based on IP only;
- Intermittent and mediated Internet of Things (IoT) reporting;
- Unique Identifier.

By dissecting core concepts like "terminal equipment", "information", "gaining access" or "storage" the EDPB ensures that these Guidelines comprehensively address ambiguities, equipping organisations with the tools needed to align their practices with the Directive while safeguarding user privacy.

2.2.3 Guidelines 01/2024 on processing of personal data based on Article 6(1)(f) GDPR

Adopted in October 2024, these [Guidelines](#) offer an in-depth exploration of legitimate interest as a legal basis for processing under Art. 6(1)(f) GDPR. The document addresses the three cumulative conditions that must be met:

- **Identification of a legitimate interest:** the interest must be lawful, specific, and present;
- **Necessity of processing:** data controllers must assess whether less intrusive alternatives could achieve the same outcome, ensuring compliance with data minimisation principles;
- **Balancing exercise:** data controllers must weigh their legitimate interest against the fundamental rights and freedoms of individuals, considering factors like transparency, safeguards, and the reasonable expectations of individuals.

Dedicated sections on specific contexts, such as fraud prevention and direct marketing, illustrate the application of these principles, providing stakeholders with insights into how to navigate this area of the GDPR.

2.2.4 Guidelines 02/2024 on Article 48 GDPR

Adopted in December 2024, these [Guidelines](#) offer critical clarity on the application of Art. 48 GDPR, which regulates access to personal data by courts and authorities in third countries, and its interaction with Chapter V GDPR.

Key recommendations include:

- **Interaction between Article 48 GDPR and Chapter V GDPR:** where data processed in the EU are transferred or disclosed in response to a request from a third country authority, such disclosure constitutes a transfer within the meaning of Chapter V. As for any transfer subject to the GDPR, there must be a legal basis for the processing in Art. 6 GDPR and a ground for transfer in Chapter V GDPR;
- **Case-by-case assessments:** generally, recognition and enforceability of foreign judgments and decisions is ensured by applicable international agreements which may provide for both a legal basis under Art. 6(1)(c) GDPR or Art. 6(1)(e) GDPR and a ground for transfer under Art. 46(2)(a) GDPR. Where no applicable international agreement exists, or the agreement does not contain a legal basis or appropriate safeguards, the EU data controller or data processor can consider other legal bases and grounds for transfer, including derogations in Art. 49 GDPR.

2.3 STATEMENTS ON LEGISLATIVE DEVELOPMENTS

Legislative developments: context and impact

The year 2024 marked significant advancements in legislative frameworks directly impacting data protection and privacy across the EU. By addressing critical and emerging challenges, the EDPB reinforced its commitment to guiding DPAs and stakeholders through the legislative landscapes.

2.3.1 Statement 1/2024 on legislative developments regarding the Proposal for a Regulation laying down rules to prevent and combat child sexual abuse

Recognising the urgency of addressing child sexual abuse online, the EDPB issued [Statement 1/2024](#), which addressed the European Commission's proposed regulation on this critical issue. While acknowledging the importance of combating such crimes, the Board emphasised the need for any measures to comply fully with fundamental rights, particularly the right to privacy and data protection.

The Statement welcomed improvements introduced by the European Parliament, including the exclusion of end-to-end encrypted communications from detection orders. However, it raised concerns over the potential for general and indiscriminate monitoring of private communications, highlighting the high error rates of certain detection technologies. The Board called for proportionality and precision in any proposed measures to ensure compliance with the EU Charter of Fundamental Rights.

This Statement reaffirmed the EDPB's commitment to protecting vulnerable individuals while safeguarding fundamental rights in legislative initiatives.

2.3.2 Statement 2/2024 on the financial data access and payments package

The EDPB's [Statement 2/2024](#) addressed the European Commission's Financial Data Access and Payments Package, comprising the Financial Data Access Regulation (FIDA), the Payment Services Regulation (PSR), and the Payment Services Directive (PSD3). This Statement was adopted in the context of ongoing legislative discussions on this package.

Building upon the practical experience of national DPAs, the Board pointed out to topics where further alignment with the guidelines issued by the EDPB and previous opinions of the EDPS on these proposals should be made.

In particular, the EDPB took note of the European Parliament's reports on the FIDA and PSR proposals, but considered that, with regard to the prevention and detection of fraudulent transactions, additional data protection safeguards should be included in the transaction monitoring mechanism of the PSR proposal. The Board recalled in this regard the need to ensure that the level of interference with the fundamental right to the protection of personal data of persons concerned is necessary and proportionate to the objective of preventing payment fraud.

2.3.3 Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework

In 2024, the EDPB issued [Statement 3/2024](#), which provided comprehensive insights into the role of DPAs within the Artificial Intelligence Act framework. This Statement emphasised the importance of a human-centric approach to AI technologies, ensuring the protection of individuals' fundamental rights, including data protection and privacy, amidst rapid technological advancements.

The Statement recommended that DPAs should be designated as MSAs for high-risk AI systems mentioned in Art. 74(8) of the AI Act. It highlighted the need for enhanced collaboration among DPAs and other regulatory bodies to address cross-sectoral challenges. Furthermore, the EDPB

stressed the importance of transparency and accountability in AI deployments, advocating for mechanisms to ensure compliance with the GDPR and the AI Act. In particular, the Statement highlights that a prominent role of the DPAs at national level should be recognised, due to the experience and expertise gathered by them in working out guidelines and best practices and carrying out enforcement actions on AI-related issues with respect to the processing of personal data at both national and international level.

Furthermore, the Statement highlighted the need for enhanced collaboration among DPAs and other regulatory bodies to address cross-sectoral challenges.



"In view of the digital transition, the publication of the AI Act surely constitutes one of the milestones that will shape Europe's digital landscape in the future. It is certain that DPAs will play a crucial role to safeguard rights and freedoms of individuals when personal data are processed in the context of AI."

**Dr. Matthias Schmidl
Head of the Austrian Data Protection Authority**

2.3.4 Statement 4/2024 on the recent legislative developments on the Draft Regulation laying down additional procedural rules for the enforcement of the GDPR

Adopted at the October 2024 plenary, the EDPB's [Statement 4/2024](#) on the recent legislative developments on the Draft Regulation laying down additional procedural rules for the enforcement of the GDPR, supported the introduction of procedural rules to harmonise the enforcement of the GDPR across countries. This Statement emphasised the need for clear and consistent rules to

streamline enforcement processes and recommended further addressing specific elements of the regulation to achieve the objectives of streamlining cooperation between authorities and improving the enforcement of the GDPR.

The Board highlighted the importance of ensuring adequate resources for DPAs to implement these procedural rules effectively. It also called for practical measures to support DPAs in managing cross-border cases, thereby promoting consistency and efficiency in enforcement.

By advocating for procedural harmonisation, this Statement represents a significant step towards strengthening the GDPR's framework and ensuring the consistent application of data protection standards throughout the EU.

2.3.5 Statement 5/2024 on the Recommendations of the High-Level Group on Access to Data for effective Law enforcement

Adopted in November, the [Statement 5/2024](#) on the recommendations of the High-Level Group (HLG) on access to data for effective law enforcement underlines the importance of safeguarding fundamental rights when law enforcement agencies access personal data. While the EDPB supports the goal of ensuring effective law enforcement, it points out concerns over certain recommendations that could potentially lead to serious intrusions on fundamental rights, particularly privacy and family life.

The EDPB notes positively that the recommendation may contribute to creating a level playing field on data retention. However, it raises concerns that a broad, general obligation for service providers to retain data in electronic form could significantly interfere with individual rights. The Board questions whether this would meet the requirements of necessity and proportionality under the Charter of Fundamental Rights of the EU and the CJEU jurisprudence.

Furthermore, the EDPB stresses that recommendations relating to encryption should not hinder its use or reduce its effectiveness. For example, introducing a client-side process that allows remote access to data before encryption or after decryption would undermine the effectiveness of encryption. Preserving the protection and effectiveness of encryption is critical, not only for respecting private life and confidentiality but also to safeguard freedom of expression and foster economic growth, both of which rely on trustworthy technologies.

2.3.6 Statement 6/2024 on the Second Report on the Application of the General Data Protection Regulation - Fostering Cross Regulatory Consistency and Cooperation

During its December 2024 plenary, the EDPB adopted the [Statement 6/2024](#) on the second report of the European Commission regarding the application of the GDPR.

The EDPB welcomes the reports from both the European Commission and the Fundamental Rights Agency, underlining the importance of legal certainty and coherence between digital legislation and the GDPR. It stresses the need for clear and consistent enforcement of the GDPR in the context of the EU's evolving digital landscape. The Board has highlighted its ongoing initiatives, including efforts to clarify the relationship between the GDPR and other critical legislation such as the Artificial Intelligence Act, or those derived from the EU Data Strategy, and the Digital Services Package.

Furthermore, the EDPB confirmed its commitment to enhancing content tailored for non-experts, small and medium-sized enterprises (SMEs), and other relevant groups, to ensure better understanding of data protection principles.

Finally, the Board calls for additional financial and human resources to address the growing complexity of data protection challenges and its expanding responsibilities. These resources are vital for enabling DPAs and the EDPB to continue their work effectively, ensuring high standards of data protection across the EU.

2.4 STAKEHOLDER CONSULTATION

The EDPB upholds its commitment to fostering transparency, inclusivity, and collaboration by actively engaging with stakeholders. These engagements enhance the relevance and practicality of its guidance.

2.4.1 Public Consultation on Guidelines

Public consultations serve as a vital tool for integrating stakeholder perspectives into the EDPB's regulatory framework. By inviting feedback from organisations, advocacy groups, and individuals, the EDPB ensures that its guidelines are aligned with practical realities. Every submission is thoroughly evaluated, and accepted contributions are incorporated into the final documents, reflecting the EDPB's commitment to participatory governance.

In 2024, the Board finalised key consultations that were launched earlier:

- The public consultation on **Guidelines 02/2023** concerning the **Technical Scope of Article 5(3)**

- of the ePrivacy Directive concluded in January 2024;
- Guidelines 01/2024 on the processing of personal data based on Art. 6(1)(f) GDPR were completed following a comprehensive consultation;

Additionally, in 2024 the EDPB launched another consultation on **Guidelines 02/2024 on Article 48 GDPR**, which closed in January 2025, further underscoring the EDPB's dedication to continuous stakeholder involvement.

2.4.2 Stakeholder Events

Stakeholder events are pivotal in fostering dialogue and knowledge exchange on emerging issues in data protection. These events not only strengthen the EDPB's understanding of stakeholder concerns but also provide a platform for diverse voices to shape the regulatory landscape.

Two high-profile events in 2024 highlighted the Board's commitment to addressing pressing and complex issues:

- **Consent or Pay models**

This dedicated event focused on the contentious practice of Consent or Pay models. The event fostered vibrant discussions among a diverse audience, including consumer rights advocates, data protection experts, and industry representatives. Key debates revolved around how these models could comply with the GDPR principles, particularly in ensuring that consent is freely given, and alternatives are genuinely equitable.

- **AI Models and GDPR compliance**

Another major event addressed the complexities of applying the GDPR principles to AI models, particularly those subject to Art. 64(2) GDPR opinions. The event featured interdisciplinary discussions, drawing insights from academia, legal professionals, NGOs, and industry leaders. Topics ranged from the ethical implications of AI-driven data processing to the practical challenges of ensuring transparency, fairness, and accountability in AI applications.

2.4.3 Survey on Practical Application of Adopted Guidance

Following the 2023 stakeholder survey's results, in 2024 the EDPB implemented most of the recommendations provided improving the accessibility of most guidelines. For instance, in 2023 stakeholders indicated that they considered EDPB's guidance language too technical; moreover they suggested to add visualisations such as videos to provide higher clarity on more technical

sections of the guidelines. The EDPB acknowledged that and implemented a series of actions, such as creating less technical factsheets associated to guidelines, including visualisations and flowcharts to help simplify complex information and more.

In addition, in 2023 stakeholders mentioned that adding an executive summary as a standard section of every document would increase the ease of use of the guidelines. In response to that, in 2024 the EDPB included an executive summary to all guidelines to provide a quick overview of the most important points. Additionally, one of the guidelines adopted before public consultation in 2024 - on legitimate interest - featured a [factsheet](#) for easier reference. To further enhance clarity, the guidelines on legitimate interest include eight examples. In response to the request made by stakeholders in 2023 for referencing academic work in the guidelines, in 2024 the EDPB made sure to include relevant citations throughout the guidelines. A final input from 2023 was to receive guidance on anonymisation; work on such guidance is currently ongoing showing the EDPB commitment to take into account stakeholders insights and putting them into practice through concrete initiatives.

In 2024, the EDPB conducted its seventh annual stakeholder survey under Art. 71(2) GDPR.

The survey evaluated the effectiveness and clarity of the EDPB's guidelines, opinions, and consultation processes issued throughout the year. It aimed to determine the practical utility of these resources in interpreting the GDPR's provisions and to identify opportunities for enhancing the support provided to organisations and individuals navigating the EU data protection framework.

Survey participants included academics specialising in data protection and privacy rights, legal professionals, business and industry representatives, members of non-governmental organisations and experts from related fields, ensuring a comprehensive range of perspectives was captured.

Among the guidelines most frequently consulted were [Guidelines 01/2024 on processing of personal data based on Article 6\(1\)\(f\) GDPR](#) and [Guidelines 02/2024 on Article 48 GDPR](#). Stakeholders generally acknowledged these guidelines as helpful resources, providing valuable interpretations of provisions of the GDPR and offering actionable guidance. At the same time, a limited number of stakeholders suggested that certain topics could benefit from more explicit analysis or additional guidance, allowing stakeholders to better understand and navigate challenging scenarios.

Opinions issued by the EDPB also received focused attention from stakeholders, especially [Opinion 08/2024 on](#)

[Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms](#), along with [Opinion 22/2024 on certain obligations following from the reliance on processor\(s\) and sub-processor\(s\)](#) and [Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models](#). While many stakeholders found these opinions helpful in interpreting the GDPR, some respondents highlighted areas where they felt some clarification could further enhance their utility. With regard to the opinion on “consent or pay” models, some respondents suggested elucidating how to ensure that consent remains truly “free” when individuals must choose between accepting tracking or paying a fee – namely, how to guarantee that users can decide without undue pressure or economic constraints making tracking the de facto only viable option. They also asked to approach carefully any introduction of new definitions, to avoid unintended impacts on regulatory consistency and clarity. Furthermore, stakeholders encouraged the EDPB to indicate more precisely how any new definitions introduced within the opinion might affect user autonomy, transparency obligations, and reference to existing legal frameworks. According to these respondents, such specificity would bolster both regulatory consistency and the provision of practical, hands-on guidance.

Stakeholders reported primarily accessing EDPB documents via direct search on the EDPB website, complemented by social media channels and informal recommendations. Most indicated regular usage of the guidelines and opinions, generally consulting them monthly or in response to specific issues. To enhance accessibility and ease of use, stakeholders recommended minor improvements, such as consistently including executive summaries. They also advocated for timely official translations, emphasising their importance for applicability across various jurisdictions and stakeholders who operate in multilingual contexts.

Public consultations and stakeholder workshops organised by the EDPB were broadly acknowledged and appreciated. Positive feedback highlighted the well-balanced timeline of consultations, aligning adequately with documents’ complexity. At the same time, stakeholders recommended that consultation periods reflect the technical nature and length of documents. Workshops were praised for promoting inclusive dialogue; however, stakeholders suggested improvements to the structure of the sessions, recommending additional opportunities for written input and clearer synthesis of workshop outcomes to maximise effectiveness.

Overall, the 2024 stakeholder survey affirmed widespread appreciation for the structured presentation, practical

examples, and clarity provided by EDPB guidance, alongside measured suggestions for enhancement. Stakeholder insights underscore the importance of maintaining clear, consistent, and accessible guidance to support effective implementation and compliance with the GDPR across diverse organisational contexts. The EDPB values the constructive feedback provided and will thoughtfully consider these recommendations in future guidance and consultative practices.

2.5 REPRESENTING THE EDPB WORLD-WIDE

In 2024, the EDPB participated in key international fora, fostering strategic collaborations, and addressing critical issues in data protection and privacy. In this way, the EDPB showcased its leadership in shaping robust data protection standards and navigating the challenges posed by rapid digital transformation.

Strategic leadership and Chair’s Engagements

Chair Anu Talus spearheaded the EDPB’s international initiatives, delivering impactful contributions at 34 high-profile speaking engagements throughout the year. These events highlighted the EDPB’s commitment to addressing evolving priorities in data protection and fostering global dialogue. Key highlights included:

- **One-stop-shop roundtable (Paris, February):** in this commemorative event, Chair Talus delivered a speech stressing the value of cross-border cooperation in addressing emerging data protection challenges;
- **In Cyber Forum (Lille, March):** during her keynote speech at this forum in France, Chair Talus examined cybersecurity and privacy issues, underscoring the need for robust safeguards and international collaboration;
- **IAPP Global Privacy Summit (Washington, April):** EDPB Chair gave a speech on “EU DPA Enforcement Priorities and Lessons Learned” offering an in-depth analysis of cross-border enforcement mechanisms and the GDPR’s global implications;
- **RSA Conference (San Francisco, May):** during the panel discussion “AI Governance & Ethics: A Discussion with Leading Voices” the Chair explored the ethical and operational challenges surrounding AI implementation;

- **Privacy Symposium Conference (Venice, June):** in her opening address, Chair Talus highlighted the significance of international collaboration in addressing privacy challenges across jurisdictions;
- **G7 Data Protection and Privacy Authorities Roundtable (Rome, October):** Chair Talus actively engaged in strategic dialogues aimed at harmonising global data protection policies and addressing cross-border regulatory challenges;
- **GPA - Global Privacy Assembly (Jersey, November):** Chair Talus participated to the 46th Global Privacy Assembly, speaking at a panel on "Defining Privacy Harms in a Modern World" and attending the closed session on "Reporting from other Partner Organizations".

New Deputy Chair appointment

During its June 2024 plenary session, the EDPB elected **Zdravko Vukić**, Director of the Croatian Personal Data Protection Agency, as Deputy Chair. Vukić succeeds Aleid Wolfsen, whose five-year mandate as Deputy Chair concluded, and will work alongside Deputy Chair **Irene Loizidou Nikolaïdou** and Chair Anu Talus.

Deputy Chair Vukić expressed his commitment to advancing the EDPB's mission, emphasising the importance of raising GDPR awareness, empowering individuals, and enhancing enforcement cooperation across the EEA. Chair Talus welcomed his appointment, highlighting the opportunity to further bolster the Board's capacity to address its growing tasks and to strengthen collaboration among national DPAs.

Deputy Chair Irene Loizidou Nikolaïdou also contributed significantly to the EDPB's international presence, participating in four high profile speaking engagements. These engagements included presentations and panel discussions at various institutes, academic forums, and policy agencies, such as CPDP in Brussels and the Spring Conference in Riga.

Broader EDPB representation

Beyond the contributions given by the EDPB Chair and Deputy Chairs, the EDPB's leadership and staff participated in 43 additional international events, encompassing expert panels, policy workshops, and collaborative discussions. These speaking events covered diverse topics, including:

- Privacy in emerging technologies such as AI and IoT;
- Enhancing regulatory cooperation to ensure seamless cross-border data flows;

- Strengthening compliance mechanisms to uphold data protection standards globally.

Driving Global Impact

The EDPB's international activities in 2024 yielded tangible outcomes, notably:

- Influencing global policy discussions on data protection and privacy through thought leadership and expertise;
- Strengthening partnerships with international stakeholders to promote the harmonisation of data protection standards;
- Sharing best practices and insights to address pressing challenges, including AI governance and digital transformation.



"With the GDPR, Europe has offered the Member States, but also the world, an extraordinary model of innovation governance. The Board can help to promote and disseminate this model, which is based on a sustainable balance between freedom and technology."

Pasquale Stanzione

President of the Italian Data Protection Authority



3. ENFORCEMENT COOPERATION AND ENFORCEMENT BY DPAS

3.1 EDPB ACTIVITIES TO SUPPORT GDPR ENFORCEMENT AND COOPERATION AMONG DPAS

Coordinated Enforcement Framework

The [Coordinated Enforcement Framework](#) (CEF) remains a pillar of the EDPB's efforts to strengthen the GDPR compliance across Europe. During its October 2023 Plenary, the EDPB selected [the right of access under Art. 15 GDPR](#) as the focus of its third coordinated enforcement action. This decision highlights the importance of the right of access. Such right allows individuals to check if their personal data is handled legally and helps them exercise other rights, like correcting or deleting their data. The EDPB's choice was driven by the significant number of complaints received by DPAs regarding this right and by the adoption in 2023 of [Guidelines 01/2022 on the right of access](#) to help data controllers comply with this right.

In 2024, the EDPB officially launched the enforcement action, with 30 participating DPAs actively engaged in the initiative across Europe. The participating DPAs contacted data controllers within their countries to assess compliance with the right of access and whether Guidelines 01/2022 were known and followed in practice. This was implemented through a variety of methods, including the distribution of questionnaires, the commencement of formal investigations where necessary, and the follow-up of ongoing enforcement actions. By utilising a harmonised approach, the CEF allows DPAs to collectively evaluate and address issues related to the implementation of this right.

The first phase of the initiative focused on gathering information and analysing national enforcement practices. A total of 1.185 data controllers were evaluated on key aspects such as response times, clarity, completeness, and overall compliance with access requests under the GDPR. Feedback from DPAs showed a mixed level of compliance across the EU. On the one

hand, some organisations, particularly those with an established internal procedure to handle access requests, demonstrated a strong awareness of their obligations. In that regard, bigger organisations were overall found to be more compliant than small and medium-sized enterprises (SMEs), with less resources. On the other hand, challenges were identified, such as inconsistent and excessive interpretations of the limits to the right of access and barriers that individuals encounter when exercising this right.

The results of this coordinated initiative have been consolidated by the EDPB into a [comprehensive report](#). This report, adopted by the EDPB Plenary in January 2025, provides an aggregated analysis of the findings, offering deeper insights into the level of compliance with the right of access across the EU. Importantly, the report highlights seven areas for improvement and delivers concrete recommendations to enhance consistency, awareness, and enforcement efforts at both national and EU levels. The annex to the report provides the detail of each action at national level.

Support Pool of Experts

The [Support Pool of Experts](#) (SPE) has continued to play a key role in strengthening the enforcement capacity of DPAs. This initiative, part of the EDPB's Strategy 2024-2027, provides critical technical expertise and tools to address complex cases and emerging data protection challenges. In 2024, nine projects have been launched to enhance the GDPR compliance and enforcement across the EU.

In 2024, the EDPB published the deliverables of seven SPE projects. One of those projects involved creating a [case digest on Security of Processing and Data Breach Notification](#). This initiative provides DPAs with a consolidated repository of decisions, offering valuable insights into recurring issues and thematic trends in enforcement. Another notable project was a new version of the [EDPB Website Auditing Tool](#), which was specifically designed to assist DPAs in evaluating website compliance, including aspects such as cookie management, transparency requirements, and consent mechanisms. The [Standardised Messenger Audit](#) project addressed the GDPR compliance challenges in widely used business communication platforms.

The SPE programme also facilitated tailored [Data Protection Officer \(DPO\) training in Croatia](#). This initiative aimed to equip DPOs with sector-specific expertise to enhance the GDPR compliance, particularly in critical sectors. The [AI Risk Assessment project](#) provided tools to address privacy risks in AI systems. For example, it looked at technologies like Optical Character Recognition (OCR), which converts scanned text into readable text, and Named Entity Recognition (NER), which identifies names, organisations, and locations in documents. Complementing this

effort, the [AI Auditing project](#) developed robust methodologies for auditing AI systems, ensuring their alignment with the GDPR principles such as transparency, fairness, and accountability.

In addition to these initiatives, the EDPB organised a Mobile Apps Bootcamp in September 2024, which built on the success of previous capacity-building events. The bootcamp brought together 50 auditors from 24 countries and the EDPS for a series of expert-led sessions. Presentations were delivered by PEReN (Pôle d'Expertise de la Régulation Numérique) and Dr. Narseo Vallina-Rodriguez, focusing on emerging risks and challenges in mobile applications. Participants also benefited from a practical training session, led by Esther Onfroy, which provided training for compliance assessments of mobile apps. The success of the bootcamp demonstrated the importance of capacity-building and cross-border collaboration in addressing new data protection challenges.

Memorandum of Cooperation with PEReN

In April 2024, the EDPB signed a Memorandum of Cooperation with PEReN, an interdepartmental office operating under the joint authority of the French Ministers of Economy, Culture, and Digital Technology. This agreement represents a significant milestone in enhancing technical collaboration to address emerging data protection challenges across Europe.

As a recognised centre of expertise in data science and algorithmic transparency, PEReN provides technical support to regulators and administrations. The Memorandum formalises a partnership aimed at advancing expertise in critical areas such as mobile application auditing, innovative data science methodologies, and ensuring transparency in algorithmic systems. A particular focus of the co-operation lies in sharing knowledge on tools to support trustworthy artificial intelligence, prioritising the monitoring and auditing of AI systems for GDPR compliance.

This partnership reinforces the EDPB's strategic commitment to leveraging technical expertise to navigate the increasingly complex data protection landscape. By fostering collaboration with specialised institutions like PEReN, the EDPB ensures that European data protection standards remain robust and adaptive in the face of evolving technological advancements.

Chat GPT taskforce

In 2024, the rapid advancements in artificial intelligence (AI) and the growing influence of large language models prompted the EDPB to take decisive action within its ChatGPT Taskforce.

The genesis of this taskforce was rooted in an absence of a unified enforcement mechanism under the one-stop-shop framework, as OpenAI had no EU establishment

prior to February 2024. The taskforce emerged as a collaborative effort to bridge gaps, ensure consistent application of the GDPR, and tackle the unique risks associated with ChatGPT's processing activities.

From its inception, the taskforce adopted an innovative and proactive approach. Multiple sessions brought together representatives from participating DPAs, fostering a dynamic exchange of information and strategies. A standardised questionnaire was developed as a foundational tool, allowing DPAs to investigate ChatGPT's practices uniformly across borders. This cohesive methodology reinforced the EDPB's commitment to ensuring data protection principles were upheld, even in the face of unprecedented technological complexities.

Key areas of investigation included data accuracy, transparency, fairness, and compliance with individual rights. The taskforce uncovered significant challenges, such as risks associated with web scraping, the processing of personal data in model training, and the generation of outputs that may not align with the GDPR principles. Preliminary findings highlighted the necessity of embedding "data protection by design and by default" into AI systems to mitigate these risks and reinforce accountability for data controllers managing personal data on an unprecedented scale.

The taskforce's work also emphasised the importance of international cooperation and expertise. By engaging with stakeholders and experts in AI, the EDPB demonstrated its capacity to adapt to evolving technological landscapes and to ensure robust enforcement mechanisms are in place for future AI-related developments.

Through the ChatGPT Taskforce, the EDPB not only reaffirmed its role as a guardian of individuals' digital rights but also set a precedent for addressing emerging challenges in the era of artificial intelligence. This initiative serves as a benchmark for future collaborations, reinforcing the GDPR's relevance in navigating the complexities of the digital age.

Secondment Programme

The EDPB Secondment Programme has evolved into a cornerstone of cross-border cooperation, fostering a spirit of collaboration and shared expertise between DPAs across Europe. Initially launched as a pilot project in 2019, the programme's success and growing popularity among countries led to its formalisation in 2024, marking a significant milestone in the EDPB's efforts to strengthen the GDPR enforcement.

In 2024, the programme facilitated 61 secondments across 27 authorities, providing participants with invaluable opportunities to deepen their expertise and enhance their operational capabilities.⁶ Following the matching of secondees with hosting authorities, a two-day training session has been held in Brussels in September 2024, organised by the EDPB Secretariat. During this training, secondees were able to learn more about the EDPB's activities, the EDPB Secretariat, the EDPS, the EU-wide enforcement and cooperation initiatives and had the opportunity to visit the EU institutions.

These secondments do not only enable participants to exchange practical knowledge and insights but also allow them to observe different enforcement approaches and best practices in diverse regulatory environments. For many, the experience extends beyond technical learning, fostering professional networks and long-lasting relationships that underpin cooperation among DPAs.

The tangible benefits of the programme resonate at both institutional and individual levels. Host authorities gain fresh perspectives and additional resources to address complex data protection challenges, while sending authorities benefit from the enhanced skills and knowledge their secondees bring back. This reciprocal value strengthens the collective capacity of the EDPB network, ensuring a harmonised and effective implementation of the GDPR requirements.

3.2 COOPERATION UNDER THE GDPR

The GDPR establishes a robust framework for collaboration among national DPAs, ensuring a harmonised approach to data protection enforcement across the EU. This cooperation is operationalised through mechanisms such as mutual assistance, joint operations, and the one-stop-shop mechanism, which collectively enhance the consistency and effectiveness of enforcement efforts.

In 2024, the EDPB's cooperative initiatives achieved remarkable milestones. The case register documented 350 cross-border cases, underscoring the high degree of coordination among DPAs in tackling complex, cross-jurisdictional data protection issues. Simultaneously, 982 procedures were initiated under the one-stop-shop mechanism, culminating in 485 final decisions. These figures reflect the operational efficiency and effectiveness of the GDPR's cooperation mechanisms

⁶ The selection process took place before the summer 2024 while the secondments have taken place or will take place until end of 2025.

in delivering harmonised enforcement and upholding individuals' rights across the EU.

The outcomes of these initiatives demonstrate the critical importance of close collaboration between DPAs. By leveraging mutual assistance and conducting joint operations, the EDPB ensures that organisations remain accountable for their GDPR obligations, irrespective of their geographical location within the EU.

This collaborative approach not only fortifies trust in the GDPR framework but also demonstrates the EU's commitment to safeguarding the fundamental rights of individuals in an increasingly interconnected digital environment.



Please note that:

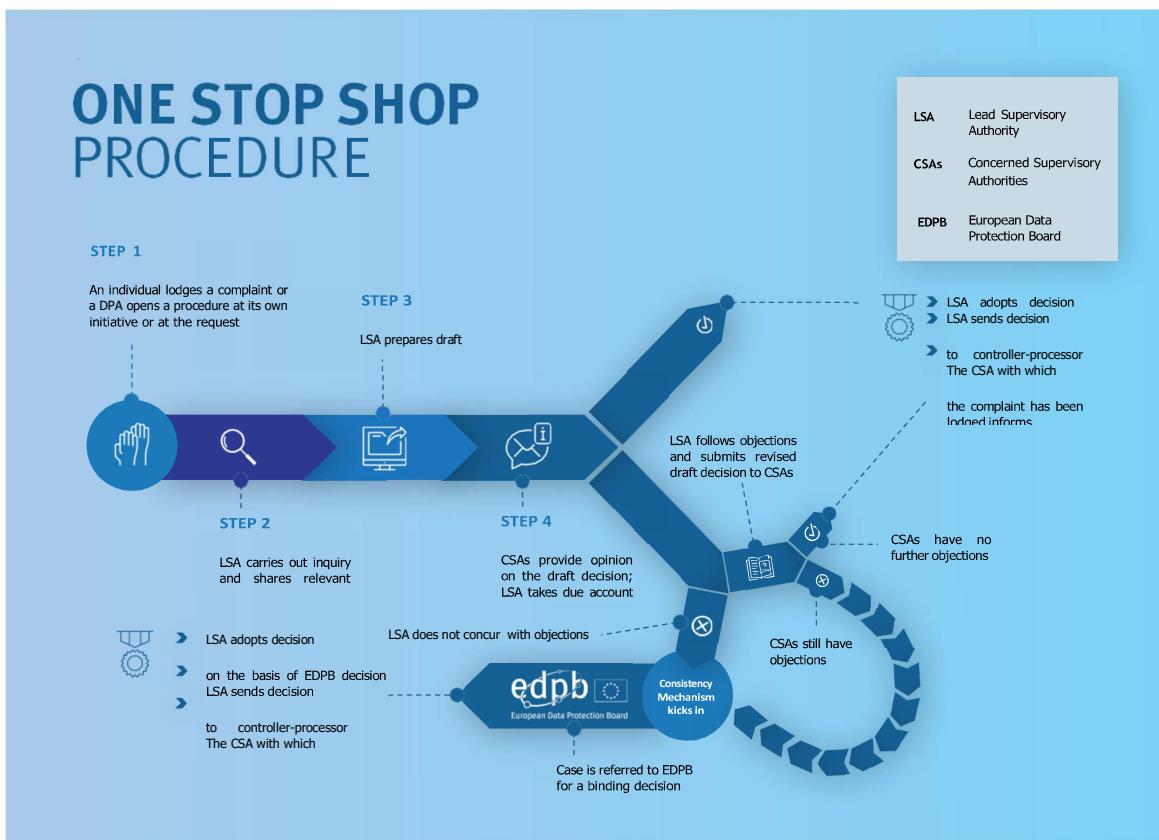
- References to case register entries in these statistics do not have a 1-to-1 correlation to the number of cross-border complaints handled per country as multiple complaints may be bundled in one case register entry, which therefore can relate to multiple cross-border cases;
- Depending on the Member State legislation, DPAs may have handled complaints outside of the Art. 60 GDPR procedure in accordance with their national law.

3.3 BINDING DECISIONS

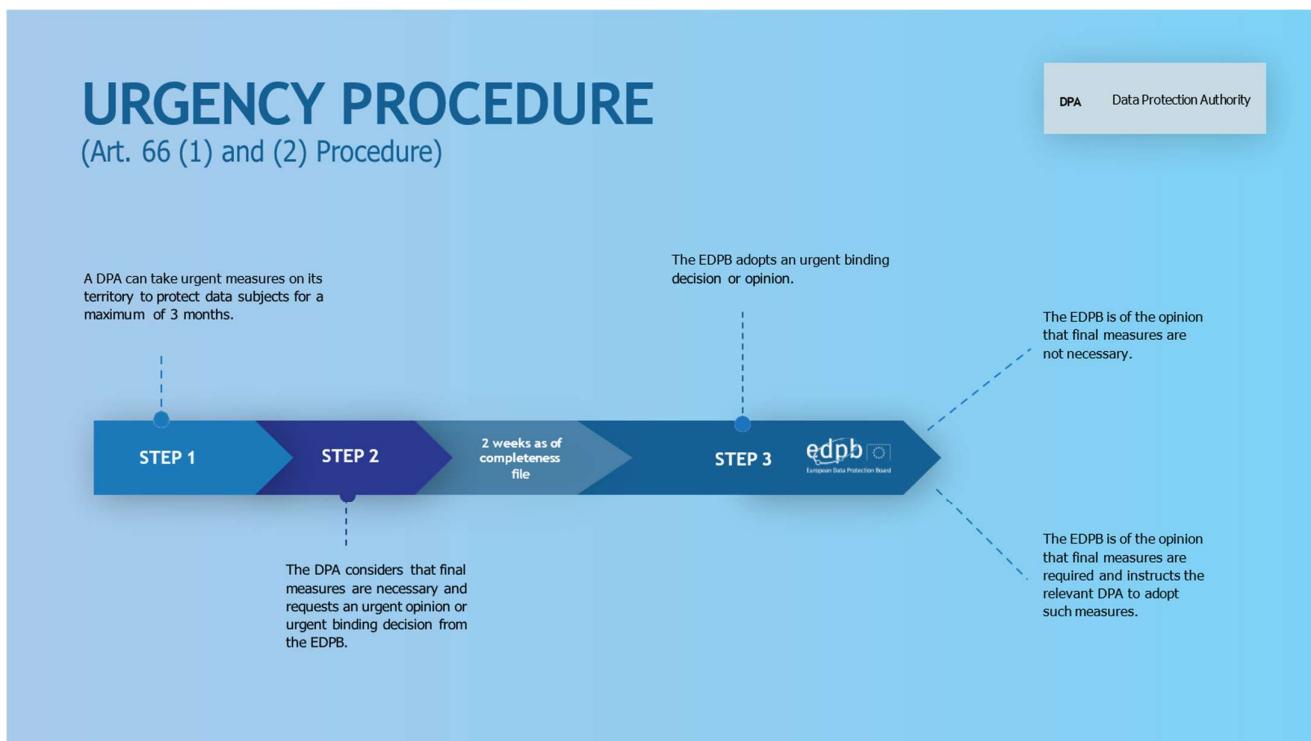
The EDPB plays a critical role in resolving disputes between DPAs and ensuring the consistent application of the GDPR through its binding decision-making powers under Art. 65 GDPR and Art. 66 GDPR. These powers help resolve disagreements in cross-border cases under the one-stop-shop mechanism. They also allow urgent action when needed.

In 2024, no binding decisions were adopted by the EDPB. This shows progress in building consensus and cooperation among DPAs. The consistent dialogue facilitated by the EDPB has allowed DPAs to resolve cases more efficiently at the national level, contributing to a more harmonised enforcement landscape across the EU.

Looking ahead, the EDPB remains prepared to exercise its binding decision-making powers as necessary to uphold the uniform application of the GDPR and address any unresolved disputes that may arise in the future.



In previous years, binding decisions have provided clarity on complex cases involving major organisations, addressing high-profile issues that impact individuals across the EU. They have also set significant precedents for GDPR enforcement, often leading to notable financial penalties and reinforcing accountability among data controllers and data processors. The urgency procedure in Art. 66 GDPR allows rapid action to maintain compliance in critical situations.



3.4 CASE DIGEST

For the third time,⁷ the EDPB commissioned a thematic case digest as part of its SPE initiative. Case digests are overviews of decisions adopted under the one-stop-shop procedure about a particular topic. The purpose of these digests is to give the DPAs and the general public, including privacy professionals, insight into the decisions adopted by DPAs following cross-border cooperation procedures.

Professor Hanne Marie Motzfeldt⁸ drafted a case digest based on the decisions adopted under the one-stop-shop mechanism regarding the right of access that are available in the EDPB register.⁹ More specifically, these decisions relate to Art. 15 GDPR ('Right of access by the data subject') and also briefly touch upon Art.12 GDPR ('Transparent information, communication and modalities for the exercise of the rights of the data subject'). The right of access of data subjects is enshrined in Art. 8 of the EU Charter of Fundamental Rights, and a large volume of decisions is available in the EDPB register on this matter.

⁷ Case digest on the right to object and the right to erasure, Alessandro Mantelero, 9 December 2022; Case digest on security of processing and data breach notification, Professor Eleni Kosta, 27 November 2023. All the previous case digests are available at https://www.edpb.europa.eu/about-edpb/publications/one-stop-shop-case-digests_en.

⁸ Professor in Administrative Law and Digitalisation at the University of Copenhagen, Ph.D. in Law.

More specifically, the SPE expert identified 185 decisions in the EDPB register, which were adopted between January 2019 and April 2024. As the SPE expert found similarities between some of these decisions, a total of 52 decisions have been selected to be included in the one-stop-shop case digest.

According to the SPE expert, the enforcement of Art.12 GDPR and Art.15 GDPR significantly supports data subjects in effectively invoking their right of access across the EEA. Almost all of the one-stop-shop decisions reviewed originate from complaints and involve almost exclusively data controllers in the private sector. Complaints often arose in a commercial context, i.e. between the data controllers and its users or customers, and revolved mainly around social media and online environments.

The one-stop-shop case digest summarises how DPAs interpret the different components of the right of access, in different contexts, namely: (1) the confirmation as to whether personal data is processed or not, (2) access to

⁹ EDPB's public register with the one-stop-shop final decisions is available at <https://www.edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions>; Annex 1 to the case digest lists the decisions relied upon and provides the link to the redacted decisions, which are available on the EDPB's public register.

and copy of such personal data, and (3) access to information about the processing, such as purpose, categories of data and recipients, duration of the processing, data subjects' rights and appropriate safeguards in case of third country transfers. In addition, the digest also analyses previous cases where exceptions and limitations to the right of access were raised by data controllers. Overall, the case digest provides useful examples on the exercise of the right of access in various contexts, for instance in the event of fake profiles or accounts which impersonate data subjects.

DPA_s do not automatically impose corrective measures in one-stop-shop decisions on the right of access. On the contrary, they often dismiss or settle the case if the matter has been resolved during the course of the proceedings.

The case digest also refers to the available guidance at EU level, and in particular, [EDPB Guidelines 01/2022 on data subject rights – Right of access](#), adopted on 28 March 2023. Relevant cases before the Court of Justice of the EU (CJEU) are mentioned. In that regard, the reviewed one-stop-shop decisions often rely on the (growing) case law of the CJEU in the field of the right of access and have recently started to refer to the EDPB Guidelines on the right of access.

3.5 NATIONAL CASES WITH EXERCISE OF CORRECTIVE POWERS

DPAs have investigative, advisory and corrective measures at their disposal to ensure entities within their countries apply data protection law correctly and consistently. Corrective measures include the following:

- Issuing warnings to a data controller or data processor where its intended processing operations are likely to infringe the GDPR;

- Issuing reprimands to a data controller or data processor where processing operations have infringed the GDPR;
- Ordering a data controller or data processor to comply with an individual's request or to bring processing operations into compliance with the GDPR;
- Imposing processing limitations, bans or fines.

In 2024, DPAs issued a number of fines, as indicated in the table below.

DPA		Num- ber of fines	Total Fines amount
Austria		63	€1 682 88
Belgium		8	€708 371
Bulgaria		25	€159 885
Croatia		38	€552 200
Cyprus		22	€133 900
Czech Republic		18	€13 882
Denmark		4	€298 657
Estonia		9	€164 100
Finland		3	€4 206 000
France		87	€55 212 400
Germany (all Länder grouped together)		416	€13 802 044
Greece		22	€4 301 249
Hungary		26	€853 788
Iceland		1	€9 961
Ireland		7	€652 029 500

DPA		Number of fines	Total Fines amount
Italy		140	€145 332 449
Latvia		14	€6 150
Liechtenstein		3	€22 911
Lithuania		13	€2 423 971
Luxembourg		1	€2 300
Malta		3	€18 000
Netherlands		16	€ 328 030 000
Norway		4	€ 63 000
Poland		25	€3 053 976
Portugal		23	€138 375
Romania		83	€371 116
Slovakia		38	€85 200
Slovenia		5	€51 000
Spain		281	€35 592 200
Sweden		6	€5 280 000
			€1 254 684 666

3.6 SELECTION OF NATIONAL CASES

This section of the Annual Report 2024 presents a non-exhaustive selection of national enforcement actions undertaken by DPAs across various EEA countries.¹⁰ The cases highlighted here illustrate the diverse regulatory responses to GDPR infringements, ranging from investigations and compliance orders to significant sanctions and fines. Many of these cases highlight recurring challenges, such as:

- Insufficient technical and organisational measures to secure personal data;
- Processing conducted without a proper legal basis, including instances where consent was not obtained;
- Unlawful processing of special categories of personal data (e.g. health data);
- Failure by data controllers to provide clear information on their processing activities and to uphold individual rights, such as the right to erasure and the right of access;
- Lack of notification of data breaches or inadequate assessment of the associated risks.

Several of the cases presented were resolved through the one stop shop cooperation mechanism, reflecting the coordinated effort at both national and European levels to ensure consistent application of the GDPR. While this selection does not examine all enforcement actions, it demonstrates the strong commitment of national DPAs to safeguard individuals' digital rights.

3.6.1 AUSTRIA

In 2024, the AT DPA performed 647 investigations, received 3.491 complaints and adopted 63 sanctions corresponding to €1.682.880 of fines. These relate among other, to unlawful processing of (sensitive) personal data due to an infringement of data protection principles (Art.5, Art. 6 and Art. 9 GDPR- most frequent infringement), infringement of data subjects' rights (Art.15 to Art. 22 GDPR - second most frequent infringement) and infringement of the obligation to cooperate with the AT DPA (Art. 31 GDPR - third most frequent infringement).

Two cases are presented in this section.

Case 1: The AT DPA imposed a fine of €1.5 million in August 2024 for the unlawful operation of a video surveillance system comprising several external and internal

cameras (violation of Art. 5 GDPR and Art. 6 GDPR). The authority took into account a recent CJEU ruling, which established that the concept of "undertaking" under Art.101 and Art. 102 TFEU must be applied when calculating GDPR fines to ensure compliance with the requirements according to Art.83(1) GDPR — effectiveness, deterrence, and proportionality (CJEU 05.12.2023, C-807/21, Deutsche Wohnen, ECLI:EU:C:2023:950). The fine was imposed on an organisation that was part of an undertaking, within the meaning of Art. 101 and Art. 102 TFEU, ensuring that the actual economic capacity of the entity was considered in determining the fine.

Case 2: In 2024, it was reported in the media that two federal states were planning an anonymised "abortion register". The AT DPA then initiated two ex officio investigations. One federal state stated that no abortion register was planned, which is why this ex officio investigation was discontinued. In the case of the other federal state, the investigations revealed that the entries in the planned abortion register were to be anonymous and aimed to identify supply bottlenecks and the risks of abortions and teenage pregnancies. However, the AT DPA had doubts as to whether anonymisation was sufficient in all cases. Likewise, the purposes of an abortion register (such as supply bottlenecks) did not appear to be compatible with the tasks of the (sole) data controller (registering medical practices or clinics). The DPA issued a warning pursuant to Art. 58(2)(a) GDPR for lack of a legal basis.

3.6.2 BELGIUM

In 2024, the Belgian DPA performed 130 investigations, received 469 complaints, issued 24 compliance orders and adopted eight financial sanctions corresponding to €708.371,00 of fines. These relate among other, to a data breach in a hospital, a data broker and the processing of biometric data.

Three cases are presented in this section.

Case 1: The Cumuleo.be case

The Belgian DPA received a cross-border complaint from the CNIL (French DPA) regarding the publication of the complainant's salary on the Belgian website Cumuleo.be. The Belgian DPA determined that the website had rightfully rejected the complainant's erasure request, as the publication of this data is necessary for exercising the right to freedom of expression and information, pursuant to Art. 17(3) GDPR. The Belgian DPA considered, in this particular instance, that the public interest in having access to this information outweighed the complainant's right to have their personal data erased from the website. Pursuant to Art. 60(3) and 60(8) GDPR, the Belgian DPA,

¹⁰ This selection of cases and figures includes those that were sent to the EDPB by the DPAs following a request to submit national enforcement news. Figures were collected between December 2024 and January 2025. The EDPB is not responsible for the accuracy of the information collected. Further cases can be found on https://edpb.europa.eu/news/news_en.

acting as the Lead Supervisory Authority (LSA) in this case, [submitted a draft decision](#) proposing to dismiss the complaint to the CNIL (with which the complaint was lodged). The CNIL raised no objections and issued its final decision on 7 August 2024.

Case 2: A cookie banner case

In September 2024, The Belgian DPA [took action against Mediahuis](#) for the unlawful use of cookie banners. The Belgian DPA had received complaints from a Dutch citizen, represented by NOYB, for four Mediahuis press websites regarding their cookie banners. The Belgian DPA reiterated that the use of deceptive design patterns is unlawful and, consequently, that the “agree and exit” button (“accept all”) should not be more prominent than another option. It recommended that both “accept all” and “reject all” options be displayed in an equivalent manner and at the same level.

The Belgian DPA ordered Mediahuis to adapt its cookie banners without using misleading button colours. In case of non-compliance after 45 days following the decision, Mediahuis must pay a €25.000 penalty per day. An appeal on the merits against this decision is still ongoing.

Case 3: A data broker case

In January 2024, The Belgian DPA [imposed a total of €174.640 in administrative fines](#) as well as corrective measures on Black Tiger Belgium, an organisation specialising in big data and data management, for various breaches of the GDPR. This penalty covers, among other things, the unfair processing of data without having proactively, individually and transparently informed the people whose data was being processed. The Belgian DPA has also noted violations linked to the exercise of data protection rights and the register of processing activities. A summary is available [here](#).

Link to annual report of Belgian DPA: <https://www.autoriteprotectiondonnees.be/citoyen/l-autorite/rapport-anuel>

3.6.3 BULGARIA

In 2024, the Bulgarian DPA performed 968 investigations, received 824 complaints, issued 38 compliance orders and adopted 25 sanctions corresponding to €159.885 of fines.

3.6.4 CROATIA

In 2024, the Croatian DPA performed 623 investigations, received 1.280 complaints, issued 153 compliance orders and adopted 191 sanctions corresponding to 38 of fines. These relate among other, to the data breach concerning owners of registered vehicles in Croatia, processing of personal data of owners of business entities, processing

of personal data via cookies and video surveillance, appointment of DPOs and in appropriate technical and organisational measures to protect sensitive data, including health data.

Three cases are presented in this section.

Case 1: The Croatian DPA received several complaints from data subjects stating that they had requested copies of their health data. However, the hospital failed to provide the copies, stating that the requested medical documentation had been irretrievably lost. As the hospital had not created backups of such personal data, access to the data subjects' personal data was entirely lost, resulting in a breach of Art. 32(1)(b) GDPR. In addition, the Agency determined that the hospital violated the following provisions of the GDPR: Art. 33(1), Art. 28(3), Art. 6(1), Art. 5(1)(e), Art. 12(1), Art. 13(1)(c), Art. 13(2)(a)(b), and Art. 38(1). As a result of these infringements, the Croatian DPA imposed an administrative fine of €190.000.

Case 2: In the investigation conducted by the Croatian DPA against an organisation whose primary business activity involves parking fee collection and parking supervision, it was determined that the data controller was processing personal data of at least 27.122 individuals for unlawful purposes and without establishing a lawful basis. This personal data was obtained through the web service of the Ministry of the Interior of the Republic of Croatia. The processing was carried out without a legal basis, in violation of Art. 5(1)(b) and contrary to Art. 6(1) GDPR. Additionally, the data controller failed to implement adequate organisational and technical measures, violating Art. 32(1)(b) and Art. 32(4) GDPR. As a result of these infringements, the data controller was imposed a fine of €80.000.

Case 3: In the investigation conducted by the Croatian DPA against a data controller whose primary business activity involves providing basic and financial data on business entities through a platform available on its website, it was determined that the data controller was processing personal data in violation of Art. 6(1)(f), in conjunction with Art. 5(1)(a) and (e) GDPR. In addition, violations of Art. 12, Art. 13, Art. 14, Art. 30, and Art. 38(3) and (6) GDPR have been identified. As a result, the rights of 170,782 individuals were infringed. For these violations of the GDPR, an administrative fine of €40.000 has been imposed.

Link to annual report of the Croatian DPA: <https://azop.hr/godisnja-izvjesca-o-radu/>.

3.6.5 CYPRUS

In 2024, the CY DPA performed 44 investigations, received 513 complaints, out of which 115 concerned spam, issued 23 compliance orders and adopted 22 sanctions corresponding to a total of €133.900,00 of fines (€9.000,00 for

five cases concerning spam). Out of the remaining 17 sanctions, 10 cases related to breach of Art. 5(1)(f) GDPR, 24(1) GDPR and 32(1) GDPR, four cases concerned Art. 12 GDPR, one case related to Art. 28(3) GDPR and Art. 35 GDPR, one case concerned Art. 5(1)(c) GDPR, and one case related to breach of Art. 15 GDPR. Two cases are presented in this section:

Case 1: Aylo Freesites Ltd

The CY DPA performed an ex officio audit of Aylo Freesites Ltd, which owns and operates a number of worldwide known adult content websites. The audit investigated the organisation's compliance with the GDPR, focusing on issues such as cookie consent, biometric data processing via a third-party, DPIAs, and data processing agreements. The Commissioner identified several violations of the GDPR, leading to a preliminary decision and subsequent fines totalling €48.000 and an additional €10.400 for the non-compliant use of cookies. Aylo Freesites Ltd responded to the findings and implemented corrective measures, resulting in a final decision that while imposing fines, acknowledged their efforts towards compliance.

In summary, Aylo Freesites Ltd. demonstrated a lack of adherence to several key data protection principles including accountability, transparency, lawfulness, fairness, data minimisation, storage limitation, data security, and the necessity of a legal basis for processing.

Case 2: State Health Services Organisation (SHSO)

The CY DPA investigated 13 data breach notifications submitted by the SHSO. 10 of these concerned loss of patients' medical files and three concerned the loss of patients' registration forms at Accident and Emergency Units. Each notification concerned a separate patient.

Even though the conditions and circumstances of each data breach were different, the investigations revealed that SHSO did not have in place appropriate technical and organisational measures (Art. 24(1) GDPR and Art. 32(1) GDPR). Its written medical file management procedure was not adequate to prevent loss of medical files and registration forms. It was concluded that patients' personal data were not processed in a manner that ensured appropriate security (Art. 5(1)(f) GDPR).

A total fine of €46.500 was imposed onto the SHSO for the reported losses: €5.000 for each of the nine medical files lost and €500 for each lost registration form. For one medical file, the Commissioner issued a reprimand since SHSO was not in a position to confirm if a file for the specific patient had been created. Reprimands were issued in two other cases, due to SHSO's delay in submitting a data breach notification to the CY DPA. In seven cases, the Commissioner ordered SHSO to communicate the breaches to the affected data subjects.

3.6.6 CZECH REPUBLIC

A fine of CZK 351 million (approximately €13.9 million) was imposed by the Czech DPA on a data controller (software organisation) for infringing Art. 6 GDPR and Art. 13 (1) GDPR. This case was dealt with through the one-stop-shop mechanism with the Czech DPA as the Lead Supervisory Authority (LSA) and all other DPAs involved as Concerned Supervisory Authority (CSA).

The Czech DPA found that the data controller collected and transferred personal data of the users of its antivirus software and its browser extensions to its sister organisation without due legal title for such processing at least during a period between April and July 2019. The transferred data related to roughly 100 million users and comprised especially pseudonymised internet browsing history of the users, tied to a unique identifier. Further, the LSA found that the data controller misinformed its users (individuals) about the said data transfers, as it claimed that the transferred data were anonymised and used solely for statistical trend analytics. The LSA concluded that internet browsing history, even if not complete, may constitute personal data, since re-identification of at least some of the data subjects could occur. The data controller's infringement is even more serious considering that it is one of the foremost experts on cybersecurity that offers tools for data and privacy protection to the public.

Link to annual report: <https://uoou.gov.cz/media-publikace/ke-stazeni/vyrocní-zprávy>

3.6.7 DENMARK

In most EEA jurisdictions, DPAs have the power to issue administrative fines. In Denmark, however, this is not the case. Instead, data protection law infringements may – taking into account the seriousness of the offence – be reported by the Danish DPA to the police. After the police has conducted an investigation to determine whether charges should be filed, the Court then decides on any possible fines. In 2024, the Danish DPA performed 518 investigations, received 1.777 complaints, and proposed (by own volition) four sanctions of at least €2.98 million in fines. Two key cases are worth mentioning in this section.

Case 1: In the first case, the Danish DPA has reported a municipality to the police for violating Art. 32 GDPR. The municipality had not encrypted up to 300 computers on which personal data was at risk of being processed. Three of the computers were stolen and they contained personal data of confidential and sensitive nature about children. It was noted in the case, that the Danish DPA believes that encryption is a basic security measure that is relatively easy and not very expensive to implement. The police are now conducting an investigation to determine whether charges should be filed, and if that is the case the Court will then decide the amount of the fine. The Danish DPA has recommended a fine of €26.000.

Case 2: In the second case, the Danish DPA decided to initiate a general investigation regarding private sector data controllers' supervision of their data processors. The investigation led to a private hospital being reported to the police for failing to supervise their three data processors to the required extent and thereby violating the principle of responsibility according to Art.5(2) GDPR. The assessment was that the private hospital was not able to ensure and demonstrate that personal data was processed in accordance with the general principles of the Art. 5(1) GDPR. The Danish DPA has recommended a fine of €200.000.

3.6.8 ESTONIA

In 2024, the Estonian Data Protection Inspectorate (EDPI) received in total 733 complaints and 184 data breach notifications affecting over 910.000 individuals. The EDPI issued 116 compliance orders, conducted 73 own initiative inspections and adopted nine sanctions corresponding to €164.100 in fines and penalty payments. In this section three cases are presented:

Case 1: The EDPI issued a fine of €85.000 to Asper Biogene OÜ. The offence consists of two misdemeanours. The first offence consists of inadequate security measures for processing personal data. For failing to ensure the security of processing of personal data in accordance with the requirements of the GDPR, the EDPI imposed a fine of €80.000. The second offence is the breach of the duty to avoid conflicts of interest in the appointment of a data protection officer or data protection specialist (DPO) and the duty to appoint a competent DPO. For that the EDPI issued a fine of €5.000.

Case 2: In 2024, the Estonian DPA also dealt with a case concerning the Viljandi Hospital where employees were asked to provide a urine sample in order to reveal the individual responsible for the theft of medicine from the hospital's medicine cabinet. The Estonian DPA issued a fine of €40.000 to the Viljandi Hospital. The Viljandi Hospital appealed against the fine decision and was successful at first instance, which the EDPI is appealing.

Case 3: Lastly the EDPI has an ongoing supervision for a data leakage that included approximately 700.000 files with personal and health data. It took place in the beginning of 2024 and was one of the biggest leakages of all time for Estonia with files consisting sensitive data.

3.6.9 FINLAND

In 2024, the Finnish DPA conducted 9 audits, received 1.932 complaints, issued 9 compliance orders and adopted 3 sanctions corresponding to €4.206.000 in fines. The fines relate to defining a storage period for customer data, lawfulness of processing, and neglecting data security. Three cases are presented in this section.

Case 1: An administrative fine of €2.4 million was imposed on Posti for unlawful processing of personal data (Art. 6(1) GDPR). The organisation had automatically created an electronic mailbox for customers without a separate request and was processing personal data on the basis of a contract. The contract included a wider set of services. The Finnish DPA considered that the service requested by the customer could have been provided without the automatic creation of an electronic mailbox. The organisation did also not inform its customers clearly about the activation of the mailbox, and there were technical settings in the service that did not meet data protection requirements. The organisation was reprimanded for the shortcomings and was ordered to correct its unlawful practices (Art 5(1)(a) GDPR, Art. 12(1) GDPR, Art. 13(1)(c) GDPR and Art. 25(1) GDPR). Two cases are presented in this section.

Case 2: The Finnish DPA imposed an administrative fine of €856.000 on the online retailer Verkkokauppa.com Oyj because it had not specified the storage period of customer account data (Art. 5(1)(e) GDPR). The organisation's practice of requiring the creation of a customer account to make online purchases also violated data protection law. The organisation was ordered to specify an appropriate storage period for customer account data and rectify its practice of mandatory registration (Art. 5(1)(e) GDPR and Art. 25(2) GDPR). The organisation was also reprimanded.

Case 3: The loan comparison provider Sambla Group was issued an administrative fine of €950.000 for data security neglect (Art. 5(1)(f) GDPR). Due to poor data security in the loan comparison services, the contents of customers' loan applications had been accessible to third parties through personal links. The organisation was ordered to cease processing the personal data its electronic services when the seriousness of the issues became apparent in March 2024. In December 2024, a fine was imposed on the organisation, and it was reprimanded for its data protection shortcomings (Art. 5(1)(f) GDPR, Art. 25 GDPR and Art. 32 GDPR). It was also ordered to notify its customers of the data breach.

3.6.10 FRANCE

In 2024, the French DPA performed 321 investigations, received a total of 17.193 complaints and closed 15.266 complaints, issued 180 compliance orders, 64 reprimands and a total of 87 sanctions corresponding to €55.2 million of fines. Under the GDPR only, it adopted 60 sanctions corresponding to €3.7 million of fines. These relate among other, to rights of individuals, legal basis, retention periods or security of personal data. This section emphasizes two significant cases.

Case 1: On April 4th 2024, the CNIL fined HUBSIDE.STORE €525.000 for having used data supplied by data brokers

for commercial prospecting purposes, without ensuring that the individuals concerned had given their valid consent (LSA: France; CSA: Belgium, Italy, Portugal, Spain).

Case 2: On 5 December 2024, the CNIL imposed a fine of €240.000 on KASPR since it collected contact details of users on LinkedIn, even if they previously masked them (LSA: France; CSA: all DPAs)

3.6.11 GERMANY

There are both national (federal) and regional DPAs in Germany. Three cases are highlighted in this section.

Case 1: The Bavarian DPA has concluded its investigation into the processing of biometric data by the organisation "Worldcoin" with an initial order. "Worldcoin" offers a digital service for human verification and a cryptocurrency, which, among other things, is based on blockchain technology. At the center of its concept is the so-called World ID, which is intended to provide proof that a stakeholder is a unique human being. Despite the improvements already initiated, further adjustments are necessary. The organisation has been ordered, among other things, to implement a deletion procedure in compliance with the GDPR regulations. In addition, "Worldcoin" is required to obtain explicit consent for certain processing steps in the future. Furthermore, the DPA has mandated the deletion of certain datasets that were previously collected without sufficient legal basis.

Case 2: The DPA of Lower Saxony responded to numerous complaints and conducted spot checks on 17 branches of 10 fitness companies and investigated additional gyms that stood out for specific reasons. The review focused on video surveillance systems, information obligations, and other formal requirements. In some cases, the DPA identified serious data protection violations and imposed fines. Three companies unlawfully monitored training areas, seating areas for customers, and employee spaces within their gyms. Additionally, two companies improperly filmed areas outside their premises. In another case, the DPA imposed a fine due to various technical-organisational deficiencies. For instance, unencrypted data backups were stored on a USB stick attached to the managing director's keychain and in the private residence of an employee.

Case 3: The Hamburg DPA audited companies with a strong market presence in the field of credit collection services. The companies were sent detailed questionnaires and were asked to provide documents such as the directory of processing activities, lists of security measures, and sample letters used. Following the written examination some companies were checked at their business premises. In the case of one organisation a six-digit number of data records with personal data had been stored without a legal basis, some of them five years

after the legal retention period had expired. The Hamburg DPA penalised the violation with a fine of €900.000.

3.6.12 GREECE

In 2024, the Greek DPA conducted four on-site inspections, received 1.820 complaints, issued 18 orders and imposed sanctions in 22 GDPR cases amounting to €4.3 million in fines, relating to, inter alia, security of processing, data breach, lawfulness, fairness and transparency, integrity and confidentiality, DPIAs, records of processing activities, data protection by design, responsibility of the data controller and cooperation with the DPA.

In the following section three cases are presented:

Case 1: In April 2024, the Greek DPA imposed a €175.000 fine and issued a compliance order to the Ministry of Migration and Asylum for violations related to the "Centaur" and "Hyperion" systems used in the reception and accommodation facilities of non-EU country nationals on the Aegean islands. The Greek DPA found a lack of cooperation on the part of the Ministry, as data controller, and further considered that the required DPIAs carried out by the Ministry were substantially incomplete and limited in scope, and that serious shortcomings remained as regards the Ministry's compliance with certain provisions of the GDPR in relation to the implementation of the systems in question.

Case 2: In May 2024, the Greek DPA imposed a fine to the Ministry of Interior (€400.000) after a major data leak involving expatriate voters' personal information. The investigation, which began after numerous complaints about unsolicited political communication via e-mail on an initiative related to the European elections by one of the data controllers, revealed unauthorised transfer of data, including email addresses and telephone numbers, outside the Ministry, leading to multiple infringements of the GDPR. In addition to the fine, the Ministry has been instructed to implement corrective measures to ensure compliance with the GDPR regulations within a specified timeframe. A second data controller involved in the case was also fined (€40.000) for the GDPR violations and ordered to delete unlawfully processed data.

Case 3: In September 2024, the Greek DPA imposed a total fine of €150.000 to the Ministry of Citizen Protection for issues arising from the introduction of the new type of identity cards for Greek citizens. In particular, the Greek DPA identified shortcomings on the provision of information to the data subjects, while it further concluded that the required DPIAs was carried out belatedly and had deficiencies. The Greek DPA clarified that the validity of the identity cards is not in question, but nevertheless it emphasised that the national legal framework concerning the content of the new type of identity cards for Greek citizens should be updated and codified.

3.6.13 HUNGARY

In 2024, the Hungarian DPA issued fines for a total of €853.788. Three cases are presented below:

Case 1: Record fine levied on the public education informatics system operator (eKréta)

eKréta is a software development and advisory organisation, dealing with the public education IT system (KRÉTA system). The databases of the KRÉTA system contain personal data of all students, parents and teachers, i.e. approximately 47 million data in the case of students, 7.5 million in the case of parents and 6.5 million in the case of teachers. eKréta is the data processor concerning the operation of the KRÉTA system. eKréta received notifications from several institutions, according to which those institutions' employees received a message with a malicious code link from the KRETA system. During the investigation of those notifications, one of eKréta's employees opened an infected element and as a result, eKréta became the victim of a phishing attack. The concerned employee's passwords and entry codes were changed, access permissions were deactivated, and the employee's computer was disconnected from the network and replaced. Thereafter eKréta closed the case. However, the concerned employee's login data were synchronised to his Google account, so the hacker remained in the internal systems through an open session. eKréta learnt about the continued existence of the attack and the possibility of a data breach only months later, following a message from the hacker on the internal communication platform. eKréta launched the notification of the data breach to the HU DPA only three days later.

The HU DPA learnt about the data breach from the media on the same day when the hacker sent the message to eKréta on the internal communication platform. The Authority launched an ex officio inspection, which was turned into an ex officio authority procedure following the subsequent media reports and the data breach notification. During the procedure, an on-site inspection was carried out at eKréta's Head office, and an IT expert opinion was prepared. As a result, the HU DPA levied on the data processor a fine of HUF 110 million (ca. €275.000) and won the subsequent Court case, in which the Court fully approved the Authority's decision.

Case 2: Irregular data processing of citizens'IDs in a large-scale energy efficiency programme

The data controller launched a countrywide LED exchange programme advertised to the general public under the energy efficiency obligation scheme. The programme targeted households i.e. natural persons. Under the programme, following an online registration and the conclusion of an energy efficiency agreement, applicants were entitled to LEDs free of charge to exchange their old

bulbs in their households to new, modern LED light sources. In order to register to the database, natural persons had to submit their personal data and, in addition, they had to upload both sides of their identity card and the card certifying their address. Most data collected were not necessary and appropriate for the purpose of data processing. At the same time, the data protection notice contained false data and was not easily accessible, while the relevant information of the data processing was incorporated in the general terms and conditions forming part of the concluded energy efficiency agreement. Moreover, the information therein concerning the rights of the data subjects were contrary to the GDPR. In addition, there was no technical solution in place to avoid downloading applicants' collected personal and it was not clear whether inactive users/former employees still had access to the database. The data controller intended to keep the collected personal data for an unlimited period of time, but permanently deleted the data earlier marked for deletion during the procedure.

The HU DPA ordered the data controller to align its data processing activities with the laws and levied a fine of HUF 75 million (ca. €187.500). The data controller contested the Authority's decision, and currently the case is pending before the court.

Case 3: CCTV overseeing employees in a McDonald's restaurant

The HU DPA received a complaint stating that in a McDonald's restaurant the CCTV surveillance system stored recordings for more than two weeks. Moreover sound recording was also taking place in addition to live video recording. Senior managers shared recordings of employees with each other in Messenger groups. According to the complaint, the employees were not informed about the CCTV surveillance and their consent was not requested. The HU DPA investigated the statements in the complaint and carried out an on-site visit at the concerned restaurant. It was established that the rest area of the restaurant designated for the employees during their break was under continuous camera surveillance and that there is no uniform and easily accessible information for employees available about the data processing. In addition, the storage period of the camera footage was not proportionate to the purpose of the data processing. As a consequence, the HU DPA called on the restaurant to align its data processing with the laws and levied a penalty of HUF 30 million (ca. €75.000).

3.6.14 ICELAND

In 2024, the Icelandic DPA performed 14 investigations, received 116 complaints, issued seven compliance orders and adopted one sanction corresponding to approximately €9.961 of fines. Two cases are presented in the following section:

Case 1: In a national case, the Icelandic DPA imposed an administrative fine of approximately €9.961 against a private organisation, Stjarnan ehf., and ordered the organisation to take corrective measures.

The case concerned the use of surveillance cameras at the complainant's workplace. The data controller argued that the organisation had legitimate interests in processing the personal data and that it was necessary for security and asset protection purposes. The investigation revealed that at the time in question, the complainant's supervisor viewed the footage of the surveillance camera at the workplace on two occasions, took screenshots and noted comments on the complainant's procedures and behaviour at work.

The Icelandic DPA found the data controller did not demonstrate the necessity for such extensive processing of personal data and therefore the processing was in breach of Art. 5(1)(a) GDPR, Art. 5(1)(b) GDPR, Art. 5(2) GDPR and Art. 6(1) GDPR, as well as Art. 9 GDPR and Art. 14(1) of the Icelandic Act no. 90/2018, on Data Protection and the Processing of Personal Data.

Case 2: In a cross-border case the Icelandic DPA conducted an audit of the processing of personal data by the organisation SidekickHealth ehf. The Icelandic DPA was the LSA. Bulgaria, Finland, Germany, Italy, Luxembourg, Norway, Spain, and Sweden were CSA's.

The main activity of SidekickHealth is the operation of the mobile application Sidekick. It allows users to record data regarding their health status and subsequently receive feedback. SidekickHealth uses Google as a data processor.

The Icelandic DPA concluded that the processing agreement between SidekickHealth ehf. and Google Ireland Ltd did not comply with the first sentence of Art. 28(3) GDPR and Art. 28(3)(a) GDPR and Art. 25(3) of the Icelandic Act no. 90/2018, on Data Protection and the Processing of Personal Data. The Icelandic DPA also concluded that SidekickHealth ehf. did not take adequate measures for the transfer of personal data to third countries, allowed by a processing agreement with Google Ireland Ltd, in accordance with Art. 44 GDPR. SidekickHealth was therefore reprimanded.

3.6.15 ITALY

In 2024, the Italian DPA performed investigations into several thousands of cases. It also received 4.032 complaints and issued over 230 compliance orders. The Garante adopted over 140 sanctions corresponding to €145.332.449 of fines, relating, among others, infringements of data subject rights, unlawful telemarketing, and data breaches affecting public and private bodies.

Three cases are presented in this section.

Case 1: The Italian DPA took corrective and sanctioning measures against OpenAI in relation to the management of the ChatGPT service. OpenAI will have to carry out a six-month information campaign and pay a fine of €15 million. The Garante forwarded the procedural documents to the Irish DPA, which became LSA on 15 February 2024, in order to investigate any ongoing infringements that have not been exhausted before OpenAI had its establishment in Ireland.

Case 2: The Garante ordered Foodinho S.r.l., an organisation of the Glovo Group, to pay a fine of €5 million for unlawfully processing the personal data of more than 35.000 riders through the digital platform. The Italian DPA also issued specific requirements and prohibited further processing of biometric data (facial recognition) of riders used for identity verification.

Case 3: The Garante ordered an energy organisation to pay a fine of €5 million for serious breaches found in the processing of personal data of more than 2.300 customers in the supply of electricity and gas. The Italian DPA took action following numerous reports and complaints regarding the closing of unsolicited contracts, filled with inaccurate and outdated data of the organisation's customers.

3.6.16 IRELAND

In 2024, the Irish DPA commenced 11 inquiries, received 2.673 complaints, issued five compliance orders and adopted seven decisions corresponding to €652 million of fines. These related, among other things, to personal data breaches concerning the storage of user passwords in plaintext, processing of personal data for the purposes of behavioural analysis and targeted advertising and exploitation by unauthorised third parties of user tokens.

Three cases are presented in this section:

Case 1: Mediahuis Ireland Group Ltd (formerly Irish News and Media plc)

Date of decision: 7 June 2024

The DPC has completed a complaint based national inquiry into Mediahuis Ireland Group Ltd (MIG) processing of personal data in relation to a series of news reports in the print and online editions of three Irish newspapers. The purpose of the inquiry was to examine if any obligations on the data controller arising under Art. 5(1)(a) GDPR, Art. 5(1)(c) GDPR, Art. 5(2) GDPR, Art. 6 GDPR and Art. 9 GDPR had been engaged and, if engaged, whether MIG infringed those obligations in publishing the personal data relating to the complainant as contained in the relevant newspaper articles.

Having regard to the totality of the evidence before it, the DPC found that the exemption under section 43(1) of the

Data Protection Act 2018 applies to the reporting by MIG about which complaint was made by the complainant, and the DPC therefore dismissed the complaint under section 112(1)(b) of the Data Protection Act 2018.

For more information, you can read the summary of the inquiry at this link: [Inquiry concerning Mediaghuis Ireland Group Limited \(MIG\) - June 2024](#)

Case 2: Inquiry into Meta Platforms Ireland Limited

Date of Decision: 26 September 2024

This inquiry was launched in April 2019, after Meta Platforms Ireland Limited (MPIL) notified the DPC that it had inadvertently stored certain passwords of social media users in ‘plaintext’ on its internal systems (i.e. without cryptographic protection or encryption).

The DPC’s Decision recorded the following findings of infringement of the GDPR:

- Art. 33(1) GDPR, as MPIL failed to notify the DPC of a personal data breach concerning storage of user passwords in plaintext;
- Art. 33(5) GDPR, as MPIL failed to document personal data breaches concerning the storage of user passwords in plaintext;
- Art. 5(1)(f) GDPR, as MPIL did not use appropriate technical or organisational measures to ensure appropriate security of users’ passwords against unauthorised processing; and
- Art. 32(1) GDPR, because MPIL did not implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including the ability to ensure the ongoing confidentiality of user passwords.

The decision included a reprimand and administrative fines totalling €91 million.

For more information, you can download the full decision at this link: [Inquiry into Meta Platforms Ireland Limited - September 2024 \(PDF, 1.2 MB\)](#).

Case 3: LinkedIn Ireland Unlimited Company Decision

Date of Decision: 22 October 2024

The inquiry examined LinkedIn’s processing of personal data for the purposes of behavioural analysis and targeted advertising of users who have created LinkedIn profiles (members). This inquiry was launched by the DPC, in its role as the Data Protection Authority that is in the lead, called the Lead Supervisory Authority (LSA) for LinkedIn, following a complaint initially made to the French DPA.

The DPC’s final decision recorded the following findings of infringement of the GDPR:

- Art. 6 GDPR and Art. 5(1)(a) GDPR, insofar as it requires the processing of personal data to be lawful, as LinkedIn;
- Art. 13(1)(c) GDPR and Art. 14(1)(c) GDPR, in respect of the information LinkedIn provided to data subjects regarding its reliance on Art. 6(1)(a) GDPR, Art. 6(1)(b) GDPR and Art. 6(1)(f) GDPR as lawful bases;
- Art. 5(1)(a) GDPR, the principle of fairness.

The decision included a reprimand, an order for LinkedIn to bring its processing into compliance, and administrative fines totalling €310 million.

For more information, you can download the full decision at this link: [Inquiry into LinkedIn Ireland Unlimited Company - October 2024 \(PDF, 1.8 MB\)](#).

3.6.17 LATVIA

In 2024, the Latvian DPA performed 974 investigations, received 693 complaints, issued 26 compliance orders and adopted 14 sanctions corresponding to €6.150 of fines relating. Two cases are presented in this section.

Case 1: The National Electronic Mass Media Council (NEPLP) published an administrative penalty decision on its website, which included the name, surname, and personal identification number of a data subject. The published decision made sensitive personal data accessible to the public, violating the GDPR.

The Data State Inspectorate found that the personal identification number had been published due to an error, and NEPLP quickly removed it. However, the name and surname remained accessible on the website. NEPLP explained that the purpose of publishing decisions was to inform industry representatives and promote understanding of regulatory requirements. The Inspectorate determined that achieving these goals did not require the publication of personal data.

The Inspectorate concluded that NEPLP had violated data processing principles and required it to delete all personal data from the published decisions by a specified deadline.

Case 2: A physician assistant, using authorised access to unified health information systems, including E-Health and other information systems containing health data of individuals, unlawfully processed the personal data of several individuals. The data processing was conducted for personal purposes and was unrelated to the performance of work duties, thereby violating the GDPR and the principle of confidentiality.

The violation involved the processing of sensitive data without a legal basis, causing emotional distress to the affected individuals. The medical institution confirmed that the employee's actions were inconsistent with professional standards and legal regulations. Consequently, the employee was fined €500, considering the severity of the violation and its impact on the affected individuals.

Link to annual reports of Latvian DPA: <https://www.dvi.gov.lv/lv/publikacijas-un-pariskati>

3.6.18 LIECHTENSTEIN

In 2024, the Liechtenstein DPA conducted nine investigations, processed 50 complaints, issued nine compliance orders, and imposed three sanctions, resulting in fines totalling €22.911. These sanctions primarily addressed issues such as transparency obligations, a data breach involving special categories of personal data, and violations of data subject rights.

Two cases are presented in this section.

Case 1: A former employee filed a complaint related to Art. 15 GDPR, claiming he was granted access only to his file, which included most of his work-related documents. However, specific data appeared to be missing from the file.

The DPA clarified that a data controller must also comply with the requirements outlined in Art. 15(1) GDPR. This entails providing the data subject with all the specified information, such as the purpose of the processing, the recipients, the data retention period, and other elements listed in paragraph 1. While providing access to a digital file may satisfy the requirements of Art. 15(3) GDPR, it does not fulfil the obligations under paragraph 1.

Additionally, the data controller cited Art. 34 of the National Data Protection Act, arguing that the data was stored solely for data security and control. However, even if the data controller relies on this exception, they must inform the data subject that they are invoking the exception.

Case 2: An online health advisory service provider unintentionally exposed users' and employees' email addresses and phone numbers online due to a technical error. The organisation attributed the breach to incorrect access rights configuration.

The DPA stated that the unprotected access to sensitive data violated Art. 32 GDPR, as it compromised data confidentiality and integrity. Furthermore, the data controller was notified of the breach by an anonymous individual but failed to act or verify the report, thus constituting a violation of Art. 33 GDPR. A fine was subsequently imposed.

3.6.19 LITHUANIA

In 2024, the Lithuanian DPA imposed 13 sanction, resulting in fines up to €2.423.971. Three cases are presented in this section.

Case 1: On July 3, 2024, the Inspectorate imposed a fine of €2.3 million on online marketplace for buying, selling, and exchanging new or second-hand items. The decision followed an investigation that revealed significant violations of key GDPR principles, particularly transparency, fairness, and accountability. Specifically, it was found that the organisation: 1) Failed to adequately address data subjects' requests for erasure and provided insufficient information, violating Art. 5(1)(a) GDPR, Art. 12(1) GDPR, and Art. 12(4) GDPR; 2) Neglected to properly implement the accountability principle, breaching Art. 5(2) GDPR; and 3) Engaged in unlawful data processing practices in the context of shadow banning, violating Art. 5(1)(a) GDPR and Art. 6(1) GDPR.

Case 2: On September 19, 2024, the Inspectorate imposed a €6.000 fine on an organisation providing dental healthcare services following an investigation into a complaint. The examination revealed that the organisation violated the principle of lawfulness under Art. 5(1) GDPR by conducting video and sound surveillance within dental offices without proper legal grounds. Additionally, the organisation infringed upon the complainant's right of access under Art. 15(3) GDPR by refusing to provide the copy of the processed data upon his request.

Case 3: In 2024, the Inspectorate investigated a complaint regarding GDPR violations by an organisation managing an online database of used vehicle records. The inquiry determined that the Organisation had breached Art. 5(1) GDPR, Art. 15(1) GDPR, and Art. 16 GDPR by failing to ensure the accuracy of personal data, denying access to requested information, and unlawfully refusing to rectify inaccurate data. The Inspectorate upheld the complaint, issued a reprimand, and directed the Organisation to resolve the identified violations within a specified timeframe. However, due to the improper execution of these instructions, the Inspectorate imposed a fine of €12.000 to the organisation on November 28, 2024, for breaching Art. 58(2) GDPR.

All of the aforementioned decisions are being contested before the regional administrative court.

3.6.20 LUXEMBOURG

In 2024, the Luxembourgish DPA performed 29 investigations, received 516 complaints, issued two compliance orders including one sanction corresponding to a fine of €2.300. These two decisions relate to video surveillance systems in the workplace.

Two cases worth highlighting are presented in this section.

Case 1: The first case was based on a complaint of a data subject who was of the opinion that their employer (a municipality) violated certain provisions of the GDPR because their employer used data collected through a video surveillance system to justify the termination of their employment contract. The Luxembourgish DPA concluded that the data controller did in fact violate Art. 5(1)(b) GDPR (principle of purpose limitation) and therefore issued a reprimand to the data controller without other corrective measures. The Luxembourgish DPA does not have the power to fine the State and the municipalities in Luxembourg.

Case 2: In the second case, the Luxembourgish DPA carried out an on-site investigation in the offices of a data controller (a small private organisation) in order to find out if their video surveillance system was in compliance with the provisions of the GDPR and the national data protection law of 1 August 2018. The Luxembourgish DPA concluded that the data controller infringed several provisions of the GDPR, namely Art. (6)(1) GDPR (lawfulness of processing), Art. 5(1)(a) GDPR (principle of transparency) linked to Art. 13(1) GDPR and 13(2) GDPR (information to be provided to data subjects), Art. 5(2) GDPR (accountability principle) linked to Art. 24(1) GDPR (responsibility of the data controller), Art. 5(1)(e) GDPR (storage limitation principle) and Art. 32(1) GDPR (security of processing).

It therefore imposed a definitive limitation on processing according to Art. 58(2)(f) GDPR concerning the data processed by two specific cameras and an order to bring processing operations into compliance with Art. 5(1)(a) GDPR linked to Art. 13(1) GDPR and Art. 13(2) GDPR according to Art. 58(2)(d) GDPR. In addition to the aforementioned measures, the Luxembourgish DPA also imposed a fine of €2.300 on the data controller.

Link to annual report: <https://cnpd.public.lu/en/publications/rapports.html>

3.6.21 MALTA

In 2024, the Maltese DPA performed 793 investigations, received 882 local complaints and acted as LSA for 256 cross-border complaints, issued 112 compliance orders and adopted three sanctions corresponding to €18.000 of fines.

Two cases are worth highlighting.

Case 1: The Maltese DPA fined a private organisation €15.000 for contacting the data subject through two direct and unsolicited marketing calls. This occurred despite the organisation confirming, following a previous complaint, that the data subject's personal data undergoing

processing for direct marketing purposes had been erased and her mobile numbers were barred from the internal systems.

The investigation found that the data controller's centralised telephone system had a feature to suppress all outgoing calls marked as 'do not call back'. While this measure was deemed appropriate, sub-contracted individuals bypassed the system as instead they were using personal mobiles to make calls. As a result, the data subject's mobile numbers were contacted again after being randomly generated by the software, despite her previous objection.

The DPA found the data controller was in breach of Art. 21(2) GDPR for failing to instruct its sub-contracted individuals and for not taking adequate steps to respect the data subject's rights.

Case 2: The Maltese DPA decided that the data controller infringed the principle of fairness and the national legislation transposing Art. 13 of the LED, by failing to inform individuals that they are approaching a zone monitored by hand-held speed cameras.

The DPA ordered the data controller to display appropriate signs that must be positioned within a reasonable distance and in such a manner that the data subject could easily recognise the circumstances of the processing before approaching a zone where hand-held speed devices are used.

3.6.22 NETHERLANDS

In 2024, the Dutch DPA performed 22 investigations, handled 6.232 complaints, issued nine compliance orders and adopted 16 sanctions corresponding to €328million of fines. These relate among other, to international transfers without meeting the requirements of the GDPR to ensure the necessary level of protection, and to processing personal data without a legal basis to do so. Two cases are highlighted in the following section:

Case 1: The Dutch Data DPA imposed a fine of €290 million on Uber. The Dutch DPA found that Uber transferred personal data of European taxi drivers to the United States (US) and failed to appropriately safeguard the data with regard to these transfers. According to the Dutch DPA, this constitutes a serious violation of the GDPR. In the meantime, Uber has ended the violation.

Case 2: The Dutch DPA imposed a fine of €30.5 million and orders to end the still ongoing violations subject to a non-compliance penalty of a maximum of €5.1 million. Clearview is an American organisation that offers facial recognition services. Among other things, Clearview has built an illegal database with billions of photos of faces, including of Dutch people. The Dutch DPA warned that using the services of Clearview is also prohibited.

3.6.23 NORWAY

In 2024, the Norwegian DPA performed 18 investigations, received 902 complaints, issued 28 compliance orders and adopted four sanctions corresponding to approximately €63.000 of fines. These relate, among other, to a data breach involving sensitive information and a failure to meet the GDPR requirements on securing personal data. Two cases are presented below:

Case 1: In a national case, the Norwegian DPA imposed an administrative fine of approximately €21.500 to a municipality for violating the GDPR after confidential personal data was unintentionally made accessible in public records. The breach involved sensitive information about students, including their names, birth dates, national ID numbers, and personal details. Although the municipality reported the breach and took corrective action, the Norwegian DPA determined that they failed to meet adequate requirements of the GDPR regarding security and legal basis.

Case 2: In a national case, the Norwegian DPA imposed an administrative fine of approximately €13.000 to a university for violating the GDPR by failing to secure personal data in Microsoft Teams. A data breach that was discovered revealed that personal data from 16.000 individuals, including employees, students, and refugees, had been exposed in open Teams folders since 2018. The breach included sensitive information such as names, ID numbers, and exam details. Following the case, the university was obliged to improve procedures, ensure proper data access controls, and provide training to employees on safeguarding personal data.

3.6.24 POLAND

In 2024, the Polish DPA performed 41 investigations, received 8.056 complaints, issued 334 compliance orders and adopted 25 sanctions corresponding to €2.9 million of fines relating.

There are three cases worth highlighting presented in this section.

Case 1: The Polish DPA fined mBank over PLN 4 million (€900.000) for failing to notify customers of a data breach. On June 30, 2022, an employee of a data processing organisation mistakenly sent client documents to another financial institution. The opened envelope raised concerns about unauthorised access to sensitive data, including personal details, bank account information, and income data.

Although mBank reported the incident to Polish DPA, it did not inform affected individuals, arguing the recipient was trustworthy. Polish DPA rejected this reasoning, stressing that trustworthiness requires a well-established, long-term relationship. The breach created significant

risks to individuals, leaving them unable to protect themselves. The fine highlights mBank's systemic failure to meet the GDPR obligations.

Case 2: During a press conference, prosecutors revealed personal data of a victim in a criminal case, including sensitive information protected under the GDPR. Despite this breach, the Prosecutor's Office neither reported the incident to the Polish DPA nor informed the individual, arguing the data was part of a court ruling and disclosed within legal obligations. The Polish DPA disagreed, emphasising that even public entities must comply with the GDPR.

The President of the Personal Data Protection Office imposed a fine of €19.800 for infringements of Art. 6, 33 and 34 of the GDPR on the National Public Prosecutor's Office. In addition, he ordered the National Public Prosecutor's Office to notify the victim, in accordance with the GDPR, of the possible consequences of the breach and of the measures, applied or proposed by the controller, to minimise the effects of the breach.

The President of the Personal Data Protection Office in Poland noted the lack of legal grounds for such disclosure and stressed the importance of protecting victim data, particularly given the role of the Prosecutor's Office in upholding the law. The fine underscores the need for strict compliance with data protection regulations.

Case 3: The President of the Personal Data Protection Office imposed a fine of PLN 10.913 (€2.500) on the "Stop LGBT" Legislative Initiative Committee for violating data protection rules during a signature collection campaign. Support lists containing sensitive data, such as names, surnames, ID numbers, and addresses, were left uncured in a church.

The Polish DPA investigation revealed flaws in risk assessment and a lack of oversight over the data. The lists were publicly accessible, allowing them to be viewed, copied, or photographed. The administrator failed to foresee the risk of exposing the data to third parties and did not implement effective protective measures.

The committee attributed the situation to the spontaneity of the process. However, the Polish DPA President concluded that neglecting the GDPR obligations exposed the data to risks. The committee was instructed to notify affected individuals of the breach and implement proper safeguards.

3.6.25 PORTUGAL

In 2024, the Portuguese DPA started 1.670 investigations procedures, performed 21 inspections, received 1.221 complaints, issued one compliance order, issued 151 warnings and applied 23 fines in the amount of €138.375.

Under the GDPR only, 12 sanctions were adopted, corresponding to €88.375 of fines. These relate, among other, to the exercise of data subjects' rights, to the lawfulness of processing, to transparency obligations and to the lack of designation of a DPO.

Two cases are presented in this section.

Case 1: Following media reports of Worldcoin Foundation's activities in Portugal, the PT DPA conducted an inspection on the collection of biometric data in specific pop-up kiosks operated by its data processor, Tools for Humanity. Subsequently, the PT DPA publicly advised to carefully consider the implications before providing their biometric data. Due to a growing number of complaints, particularly regarding the collection of minors' data, without parental consent, the impossibility of deleting data and concerns about potential uses of the data, the PT DPA issued an order to the data controller to suspend the biometric data collection within Portugal, in order to safeguard the fundamental right to personal data protection, especially for minors. Worldcoin Foundation, now known as World, has not resumed operations in Portugal. After receiving information regarding the existence of an establishment of Worldcoin Foundation in Germany, the Procedure was sent to the Bavarian Authority (BayLDA).

Case 2: Following the EDPB Opinion 11/2024 on facial recognition for streamlining airport passenger flow, the PT DPA conducted an inspection at Lisbon's Humberto Delgado Airport. A team of three auditors examined the associated data processing activities, hardware, and use cases involving biometric data. To analyse thoroughly the "Biometric Experience," this assessment was performed in a laboratory setting at the data controller's facilities, ANA Aeroportos. The data controller provided satisfactory responses to inquiries and demonstrated all relevant business cases. The inspection findings have been documented and are currently undergoing legal review for the GDPR compliance.

Link to annual report of PT DPA:
<https://www.cnpd.pt/cnpd/relatorios-de-atividades/>

3.6.26 ROMANIA

Case 1: The data controller for Bucharest Municipality District 1 has been fined RON 159.000 for failing to comply with a remedial order issued by the Romanian DPA. The investigation began following concerns about potential violations of data processing laws involving an online platform used to collect personal data.

Initially, District 1 received a reprimand for not providing the requested information. A remedial plan was issued, requiring the submission of the requested data within ten days. However, when the municipality failed to comply, the DPA imposed a RON 10.000 fine.

Despite the second report's warning, the district again failed to provide the required information, leading to the imposition of a coercive fine of RON 159.000. This fine was calculated for a 53-day delay (from December 29, 2023, to February 19, 2024). Under Law no. 102/2005, the DPA is authorized to fine up to RON 3.000 for each day of delay if a data controller fails to meet an ordered corrective measure or refuses to cooperate during an investigation.

Case 2: In October 2024, the Romanian DPA completed an investigation into data controller Altex România S.A. and found violations of the provisions of Art. 32 (1)(b) GDPR and of Art. 32 (2) GDPR. The data controller was sanctioned with a fine of RON 99.516.

The investigation followed two personal data breach notifications from Altex România:

- The data controller was informed by e-mail by a third party about the fact that some accounts of the data controller's customers were published on a platform, and that the personal data of a very large number of data subjects being affected, namely: name, surname, e-mail, altex.ro account's password, information available in the customer account, such as delivery address, telephone number, order history, data related to the cards with which the online payment is made, communications in connection with the data controller;
- The data controller reported a "credential stuffing" computer attack, through repeated attempts to validate passwords on some customer accounts for placing gift cards orders; the following personal data were affected, for a significant number of data subjects: name, surname, e-mail address, customer account access password, and registered bank cards in the app/website.

The Romanian DPA found that Altex România S.A. did not implement adequate security measures. This led to the unauthorised access to the personal data of a very large number of customers.

In addition to the fine, the DPA ordered corrective measures to improve security of the processing, namely, by changing the login notification, displaying the logged in devices in the account, changing the password policy, and implementing measures to monitor the incoming and outgoing internet traffic.

Case 3: Following a complaint, the Romanian DPA found that a controller disclosed the e-mail addresses of individuals when information was distributed by email, because the recipients' addresses were not included in 'blind car-

bon copy' (BCC). This led to the disclosure of approximately 180 e-mail addresses to other recipients, thus infringing the obligations imposed by Art. 32 GDPR.

A fine of RON 24.870,5 was imposed (the equivalent of €5.000) together with the corrective measure of re-evaluation of the implemented security measures, so as to ensure a level of security adequate to the risk of the processing, especially in terms of training the persons who process data under the authority of the controller and the regular verification of compliance with the instructions sent to them.

3.6.27 SLOVENIA

In 2024, the Slovenian DPA performed 384 investigations, received 184 complaints, issued 25 compliance orders and adopted five sanctions under the GDPR, corresponding to €51.000 of fines.

These relate¹¹ to data processing without an appropriate legal basis and inadequate security of processing according to Art. 32 GDPR.

There are three cases worth highlighting which are presented in this section.

Case 1: The Slovenian DPA carried out an infringement procedure against the organisation FOVELLA d.o.o., acting as the owner of DODO PIZZA franchise in Slovenia. The DPA had previously found two breaches in the inspection proceeding, relating to unlawful CCTV inside working premises and live broadcast of these CCTV footages on the organisation's website. The Slovenian DPA decided that there is no legal basis under national legislation and Art. 6 GDPR for specific CCTV. The Slovenian DPA imposed a fine of €25.000 to the organisation for unlawful CCTV inside working premises and the broadcast of the footages via the organisation's website. The DPA also issued a reprimand for breach of national Data Protection Act and Art. 13 GDPR, as the organisation failed to inform data subjects of the data processing.

Case 2: The Slovenian DPA assessed the lawfulness of video surveillance in a primary school. It was established that the data controller was unlawfully recording the school lobby and the corridor and published an incomplete notice on the processing of personal data according to national Data Protection Law and Art. 13 GDPR. Following a notice from the DPA, the data controller re-directed the cameras to only cover the entrance to the school, as allowed by the national law, and updated the notice on the processing of the personal data.

Case 3: The Slovenian DPA received a complaint from an individual regarding the erasure of his personal data from criminal records, as the data retention period had expired. The police rejected his request and explained that Police Tasks and Powers Act provides, that after the expiry of retention periods, the criminal records data shall be blocked, and the data shall be retained for 30 years. The DPA found that a constitutional review was required to determine whether the retention period of blocked data and the method of anonymisation after the expiry of the retention period were set appropriately and whether the principles of purpose limitation, data minimisation and limitation of the retention period were respected. The Slovenian DPA has therefore suspended the proceedings and submitted a request for a review of the constitutionality and legality to the Constitutional Court.

Link to annual report of the Slovenian DPA:

<https://www.ip-rs.si/publikacije/letna-poro%C4%8Dila/>

3.6.28 SPAIN

In 2024, the Spanish DPA performed 311 investigations, received 18.841 complaints, issued 391 compliance orders and adopted 281 sanctions corresponding to about €35.6 million of fines. These relate among other, to fraud in service contracts, personal data breaches concerning large companies such as insurance, energy suppliers or telecoms. The fines concern both data protection by design and lack of measures to ensure an appropriate level of security, but also the non-compliance of data protection principles, for example the lawfulness of the processing of banks and telecoms; or the processing of special categories of personal data such as health records by employers.

Three cases are presented in this section, representative of these topics and sectors.

Case 1: PS/00216/2023

The Spanish DPA imposed a fine of €5 million on the electricity company Energía VM Gestión de Energía S.L. The company was fined €2.5 million for infringements of Art. 5(1)(a) GDPR (lack of fairness and transparency) and €2.5 million for infringements of Art. 5(2) GDPR. This procedure initiated after the Spanish DPA received complaints from customers of another electricity company (Naturgy), allegedly on behalf of their current electricity company. The controller deceived individuals to attract customers, and modify the data of the individuals in the databases of Naturgy.

¹¹ This data refers only to the GDPR, however the SI DPA also conducts proceedings and imposes measures and sanctions for infringements of the Data protection Act (ZVOP-2) and Act on the Protection of Personal Data in the Field of Criminal Offences (ZVOPOKD). Most of the infringements in these proceedings concern, among other, unlawful disclosure of personal data to unauthorised users, unlawful publication of personal data, unlawful collection of personal data, unlawful video surveillance and unlawful processing in direct marketing activities.

Case 2: PS/00145/2023

The procedure was initiated by the personal data breach suffered in a web application of the electricity distribution organisation I-DE Redes Eléctricas S.A., belonging to the Iberdrola Group.

The breach was caused by a computer attack exploiting a vulnerability in the I-DE web application and affected the confidentiality of 1.35 million I-DE customers.

A fine of €2.5 million was imposed for the infringement of Art. 5(1)(f) GDPR and another one of €1 million for infringement of Art. 32 GDPR.

The breach also affected almost 2 million customers of two other companies of the Group, as the attacker managed to violate the logical separation existing in the common database of the entities of the Iberdrola Group.

Case 3: PS/00291/2023

In the telecommunications sector, a number of important sanctioning procedures have also been carried out, such as PS/00291/2023 against Telefónica de España SAU. This case was opened as a result of the notification of a personal data confidentiality breach, in which the data affected were landline telephone numbers and equipment data of more than 1.4 million customers.

The breach occurred as a result of massive access (from 55.000 requests a day to 4 million requests and by a single user), through a web portal used by employees to access customer data.

Telefónica was sanctioned €500.000 and €800.000 for violations of Art. 5(1)(f) GDPR and Art. 32 GDPR.

Link to annual report: [Memorias | AEPD](#)

3.6.29 SWEDEN

In 2024, the Swedish DPA (Integritetsskyddsmyndigheten, IMY) performed 418 investigations, received 3.814 complaints, issued 23 compliance orders and adopted six sanctions corresponding to €5.2 million of fines relating. Two cases are presented in this section.

Case1: Wrongful use of Meta Pixel

After receiving a data breach notification from a Swedish digital bank, IMY launched an investigation. The breach concerned the banks' use of the Meta Pixel on its web site and app. The Meta Pixel was used to optimise the banks' marketing on Facebook. By mistake, the bank had activated functions in the Meta Pixel, which meant that personal data, such as account numbers and securities, had been transferred erroneously to Meta. IMY concluded that the bank had processed personal data in violation of Art. 5(1)(f) GDPR and 32(1) GDPR by failing to take appropriate

technical and organisational measures to ensure an appropriate level of security for the personal data in question when using the Meta Pixel. IMY issued a fine of approximately €1.3 million against the bank.

During 2024, IMY has carried out several additional investigations into other organisations using the Meta Pixel. Some of these have also ended up with IMY issuing fines.

Case 2: Unauthorised camera surveillance by housing organisation

After receiving a complaint, IMY launched an investigation of a housing organisation and its use of camera surveillance in an apartment building. In the building, there were cameras in the entrances to three stairwells and a basement entrance to the property. There were also several cameras in the basement, storage room, operations, laundry room, garbage room, garage and corridors to the sites. IMY found that the organisation had processed personal data in violation of Art. 6(1) GDPR and Art. 13 GDPR by conducting camera surveillance in the apartment building without proper legal basis. IMY ordered the organisation to cease all camera surveillance in the apartment building, except for the parking garage, and issued a fine of €17.375 against the organisation.

4. ANNEXES

This chapter gathers documents, opinions, and tools developed or adopted in 2024 by the EDPB. These annexes serve as a detailed reference for stakeholders and DPAs, illustrating the breadth of the Board's work in clarifying the GDPR and supporting consistent enforcement across the EU.

4.1 GENERAL GUIDANCE ADOPTED IN 2024

Guidelines adopted prior to public consultation

- [Guidelines 01/2024 on Processing of Personal Data Based on Article 6\(1\)\(f\) GDPR](#) – Adopted on 8 October 2024;
- [Guidelines 02/2024 on Article 48 GDPR](#) – Adopted on 2 December 2024.

Guidelines adopted after public consultation

- [Guidelines 01/2023 on Article 37 of the Law Enforcement Directive \(LED\)](#) – Adopted on 19 June 2024;
- [Guidelines 02/2023 on the Technical Scope of Article 5\(3\) of the ePrivacy Directive](#) – Adopted on 7 October 2024.

4.2 CONSISTENCY OPINIONS ADOPTED IN 2024

4.2.1 Art. 64(1) GDPR Opinions

Draft codes of conduct

- [Opinion 12/2024 on the draft decision of the French Supervisory Authority regarding the "Code of Conduct for Service Providers in Clinical Research" submitted by EUCROF](#) – Adopted: 18 June 2024.

Accreditation standards for certification bodies and schemes

- [Opinion 7/2024 on the draft decision of the German North Rhine-Westphalia Supervisory Authority regarding the EU Cloud Service Data Protection \(Auditor\) certification criteria](#) – Adopted: 17 April 2024;
- [Opinion 10/2024 on the draft decision of the competent supervisory authority of Sweden re-](#)

garding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 GDPR

– Adopted: 23 May 2024;

- [Opinion 18/2024 on the draft decision of the Austrian Supervisory Authority regarding DSGVO-zt GmbH certification criteria](#) – Adopted: 16 July 2024;
- [Opinion 26/2024 on the draft decision of the DE Bremen Supervisory Authority regarding the "Catalogue of Criteria for the Certification of IT-supported processing of Personal Data pursuant to art 42 GDPR \('GDPR – information privacy standard'\) presented](#) – Adopted: 2 December 2024.

Approvals of Binding Corporate Rules (BCRs)

- [Opinion 01/2024 on the draft decision of the Dutch Supervisory Authority regarding the Processor Binding Corporate Rules of the Booking.com Group](#) – Adopted: 16 January 2024;
- [Opinion 2/2024 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of the TELEFÓNICA Group](#) – Adopted: 13 February 2024;
- [Opinion 3/2024 on the draft decision of the Irish Supervisory Authority regarding the Processor Binding Corporate Rules of the Accenture Group](#) – Adopted: 13 February 2024;
- [Opinion 05/2024 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of the MAPFRE Group](#) – Adopted: 14 March 2024;
- [Opinion 9/2024 on the draft decision of the Romanian Supervisory Authority regarding the Processor Binding Corporate Rules of the Genpact Group](#) – Adopted: 23 May 2024;
- [Opinion 13/2024 on the draft decision of the Supervisory Authority of Liechtenstein regarding the Controller Binding Corporate Rules of the Ivoclar Vivadent Group](#) – Adopted: 18 June 2024;
- [Opinion 14/2024 on the draft decision of the Estonian Supervisory Authority regarding the Processor Binding Corporate Rules of the Mercans Group](#) – Adopted: 16 July 2024;
- [Opinion 15/2024 on the draft decision of the Spanish Supervisory Authority regarding the Processor Binding Corporate Rules of the AVATURE Group](#) – Adopted: 16 July 2024;

- [Opinion 16/2024 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of the AVATURE Group – Adopted: 16 July 2024;](#)
- [Opinion 17/2024 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of the FCC Group – Adopted: 16 July 2024;](#)
- [Opinion 20/2024 on the draft decision of the North Rhine-Westphalian Supervisory Authority regarding the Controller Binding Corporate Rules of the Viega Group – Adopted: 17 September 2024;](#)
- [Opinion 21/2024 on the draft decision of the French Supervisory Authority regarding the Processor Binding Corporate Rules of the Talan Group – Adopted: 17 September 2024;](#)
- [Opinion 23/2024 on the draft decision of the Irish Supervisory Authority regarding the Controller Binding Corporate Rules of the Aptiv Group – Adopted: 4 November 2024;](#)
- [Opinion 24/2024 on the draft decision of the Hesse Supervisory Authority \(Germany\) regarding the Controller Binding Corporate Rules of the Infosys Group – Adopted: 2 December 2024;](#)
- [Opinion 25/2024 on the draft decision of the Hesse Supervisory Authority \(Germany\) regarding the Processor Binding Corporate Rules of the Infosys Group – Adopted: 2 December 2024.](#)

4.2.2 Art. 64(2) GDPR Opinions

- [Opinion 04/2024 on the notion of main establishment of a controller in the Union under Art. 4.16\(a\) GDPR – Adopted: 13 February 2024;](#)
- [Opinion 6/2024 on the draft list of the Latvian SA on processing operations exempt from the data protection impact assessment requirement \(Art. 35.5 GDPR\) – Adopted: 16 April 2024;](#)
- [Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms – Adopted: 17 April 2024;](#)
- [Opinion 11/2024 on the use of facial recognition to streamline airport passengers' flow \(compatibility with Articles 5\(1\)\(e\) and\(f\), 25 and 32 GDPR\) – Adopted: 23 May 2024;](#)
- [Opinion 19/2024 on the EuroPrise criteria of certification regarding their approval by the Board as European Data Protection Seal pursuant to Article 42.5 \(GDPR\) – Adopted: 16 July 2024;](#)

- [Opinion 22/2024 on certain obligations following from the reliance on processor\(s\) and sub-processor\(s\) – Adopted: 7 October 2024;](#)
- [Opinion 27/2024 on the Brand Compliance criteria of certification regarding their approval by the Board as European Data Protection Seal pursuant to Article 42.5 \(GDPR\) – Adopted: 2 December 2024;](#)
- [Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models – Adopted: 17 December 2024.](#)

4.3 STATEMENTS ON LEGISLATIVE DEVELOPMENTS

- [Statement 1/2024 on legislative developments regarding the Proposal for a Regulation laying down rules to prevent and combat child sexual abuse – Adopted: 13 February 2024;](#)
- [Statement 2/2024 on the financial data access and payments package – Adopted: 23 May 2024;](#)
- [Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework – Adopted: 16 July 2024;](#)
- [Statement 4/2024 on the recent legislative developments on the Draft Regulation laying down additional procedural rules for the enforcement of the GDPR – Adopted: 7 October 2024;](#)
- [Statement 5/2024 on the Recommendations of the High-Level Group on Access to Data for Effective Law Enforcement – Adopted: 4 November 2024;](#)
- [Statement 6/2024 on the Second Report on the Application of the General Data Protection Regulation - Fostering Cross-Regulatory Consistency and Cooperation – Adopted: 3 December 2024.](#)

4.4 OTHER DOCUMENTS

Enforcement and Cooperation Tools

Support and Capacity Building - reports commissioned by the EDPB and drafted by SPE experts

- [Report on the extraterritorial enforcement of the GDPR](#)
- [Report on the use of SPE external experts](#)
- [Standardised Messenger Audit](#)

EDPB Annual Report 2024

- [Data Protection Officer training in Croatia](#)
- [AI Risks: Optical Character Recognition and Named Entity Recognition](#)

Taskforces

- [ChatGPT Taskforce Report](#)

One-stop-shop case digest - reports commissioned by the EDPB and drafted by SPE experts

- [One-stop-shop case digest on right of access](#)

CONTACT DETAILS

Postal address

Rue Wiertz 60, B-1047 Brussels

Office address

Rue Montoyer 30, B-1000 Brussels

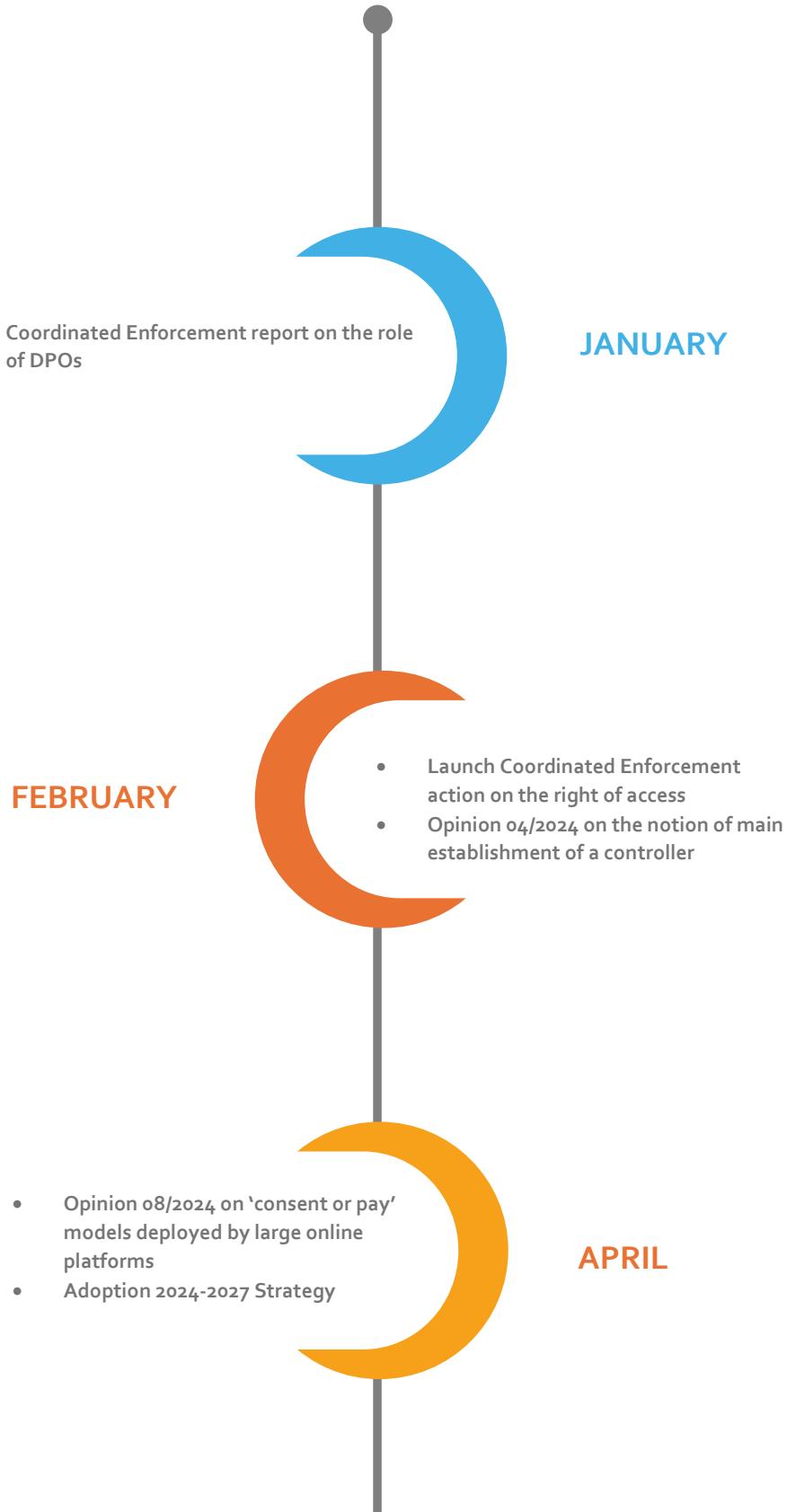
EXECUTIVE SUMMARY

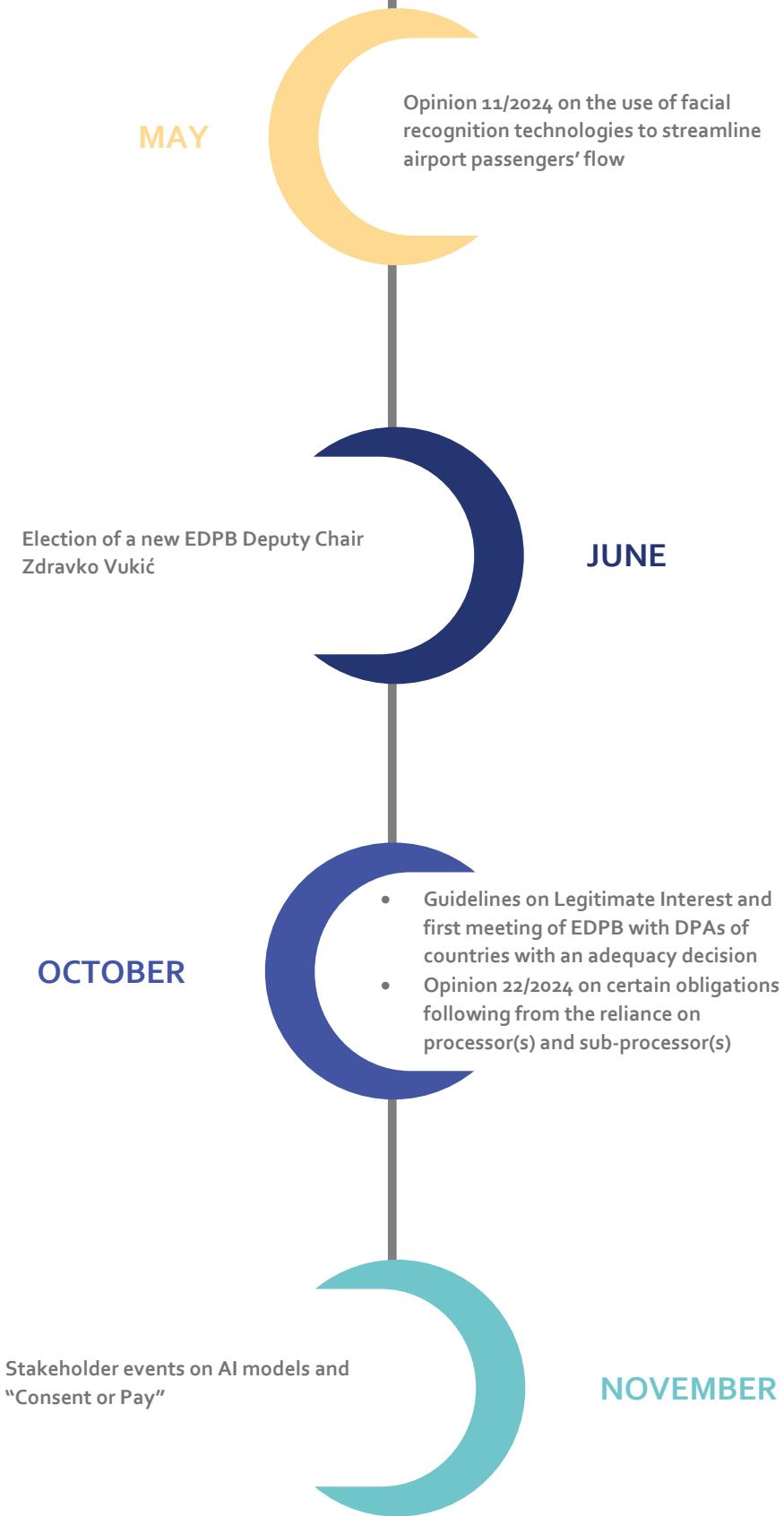
2024

PROTECTING PERSONAL DATA IN A CHANGING LANDSCAPE



HIGHLIGHTS 2024







DECEMBER

Opinion 28/2024 on AI models

INTRODUCTION

In 2024, the EDPB reaffirmed its commitment to safeguarding individuals' fundamental rights to privacy and data protection in a fast-changing digital landscape. A key milestone was the adoption of the EDPB's [new Strategy 2024–2027](#), which sets out the Board's priorities for strengthening enforcement, promoting compliance, and addressing emerging technological challenges. The strategy is built around four strategic pillars: enforcing data protection effectively, supporting compliance, enhancing cooperation, and promoting data protection in the digital age.

The [European Data Protection Board \(EDPB\)](#) continued to play a central role in providing guidance and legal advice to ensure the consistent application of the [General Data Protection Regulation \(GDPR\)](#) across the European Economic Area (EEA). In 2024, the number of consistency

opinions adopted under Art. 64(2) GDPR significantly increased, underlining the importance of this instrument in promoting early alignment on matters of general application.

To support understanding and implementation of data protection obligations, the EDPB further expanded its outreach activities. [The Data Protection Guide for Small Business](#), launched in 2023, was made available in 18 languages, and a new series of guideline summaries was developed to assist non-expert audiences in navigating key topics under the GDPR.

In parallel, the Board actively contributed to cross-regulatory cooperation by engaging with EU and international partners, including the European Union Artificial Intelligence Office and the High-Level Group on the Digital Markets Act. These efforts highlight the Board's growing role in shaping data protection within an increasingly interconnected regulatory environment.

1. THE EDPB SECRETARIAT

In 2024, the EDPB [Secretariat](#) significantly advanced its capacities to effectively respond to an increasingly dynamic regulatory landscape, reinforcing its pivotal role in upholding data protection right.

The Secretariat ensures comprehensive analytical, administrative and logistical support for all EDPB activities. It contributes specifically to drafting consistency opinions and guidance documents, and managing litigation ensuring robust support across all EDPB operations.

A noteworthy area of evolution was the Secretariat's digital transformation and enhancement of internal information systems. The Internal Market Information (IMI) system remained central, facilitating over 5.644 procedures throughout the year, a significant increase compared to previous years. To enhance the user experience, new centralised training resources and video tutorials were introduced, simplifying access to and improving the effective use of EDPB IT tools among Data Protection Authorities (DPAs).

The Secretariat supported the Board in its cross-regulatory work, cooperating closely with EU regulatory bodies such as the European Data Innovation Board and the High-Level Group on the Digital Markets Act (DMA). Moreover, the Secretariat's role in supporting the [Coordinated Supervision Committee \(CSC\)](#) increased as the tasks of CSC expanded, particularly in the preparation for supervising critical large-scale EU IT systems, including the Visa Information System (VIS) and the European Travel Information and Authorisation System (ETIAS).

Transparency and accountability continued to be essential priorities, with the Secretariat managing 38 public access requests for EDPB documents. Additionally, the Secretariat organised over 530 meetings during the year, significantly exceeding the previous year's activities.

By proactively adapting to evolving technological challenges and regulatory responsibilities, the EDPB Secretariat provided support for effective GDPR enforcement and strengthened the collaborative framework for protecting data privacy rights across Europe.

2. EUROPEAN DATA PROTECTION BOARD - ACTIVITIES IN 2024

In 2024, the EDPB significantly reinforced its pivotal role in ensuring the consistent interpretation and robust enforcement of data protection rules across Europe. In 2024, amid rapid technological advancements and increasing digital complexity, the EDPB addressed emerging data protection challenges through its guidance and consistency work. Throughout the year, the Board adopted key consistency opinions, comprehensive general guidelines and influential statements on significant legislative developments. These measures substantially contributed to ensuring a coherent regulatory framework, thereby shaping Europe's data protection landscape and reinforcing individuals' fundamental rights to privacy and data protection.

2.1 CONSISTENCY OPINIONS

Art. 64(1) GDPR Opinions

In 2024, the EDPB issued 20 opinions under Art. 64(1) GDPR, primarily addressing the approval of Binding Corporate Rules (BCRs) to facilitate secure international data transfers within multinational companies. Additionally, the Board provided clarity through opinions on draft accreditation requirements for certification bodies and code of conduct monitoring entities. These opinions were instrumental in enhancing a uniform interpretation and application of GDPR standards across Member States.

Art. 64(2) GDPR Opinions

In 2024, the EDPB adopted eight consistency opinions under Art. 64(2) GDPR, below is a selection of the most relevant ones:

- [Opinion 04/2024 on the notion of main establishment of a controller in the Union under Article 4\(16\)\(a\) GDPR](#) clarified criteria for determining a controller's main establishment within the EU. This clarification was crucial for enabling Data Protection Authorities to determine jurisdiction accurately and consistently under Art. 4(16)(a) GDPR;

- [Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms](#) emphasised essential requirements to ensure that consent provided by users remains truly voluntary and informed, thereby protecting individual autonomy and choice;
- [Opinion 11/2024 on the use of facial recognition to streamline airport passengers' flow \(compatibility with Articles 5\(1\)\(e\) and\(f\), 25 and 32 GDPR\)](#), highlighted critical compliance points such as transparency obligations, proportionality assessments, and strict safeguards required to protect sensitive biometric data and passengers' privacy rights;
- [Opinion 22/2024 on certain obligations following from the reliance on processor\(s\) and sub-processor\(s\)](#) provided clear guidance on contractual agreements, necessary oversight mechanisms, and measures ensuring accountability and GDPR compliance throughout the data processing chain;
- [Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models](#) underscored the necessity of transparency, robust explainability mechanisms and ongoing oversight to mitigate privacy risks and uphold data subjects' rights.

2.2 GENERAL GUIDANCE

In 2024, the EDPB adopted four guidelines, two of which were finalised following public consultation initiated in 2023, providing critical resources to support organisations in achieving and maintaining GDPR compliance. Notably, [Guidelines 01/2024 on processing of personal data based on Article 6\(1\)\(f\) GDPR](#) provided in-depth clarifications, including practical examples and assessment methodologies, and recommended procedural safeguards to ensure the legitimate interest balance against data subjects' rights and freedoms.

[Guidelines 02/2024 on Article 48 GDPR](#) comprehensively addressed cross-border data transfers under Art. 48 GDPR, detailing required safeguards, assessments, and mechanisms to ensure transfers align with GDPR standards, particularly focusing on international data transfers and judicial and administrative requests for data access. The guidelines offered organisations practical

strategies to navigate complex international data flows securely and compliantly.

Moreover, the EDPB adopted two additional guidelines after public consultation, reinforcing its commitment to transparency and stakeholder collaboration. This inclusive approach enhanced the applicability and practicality of guidance documents, facilitating easier compliance for businesses of all sizes.

2.3 STATEMENT ON LEGISLATIVE DEVELOPMENTS

Throughout 2024, the EDPB contributed to the law-making process by issuing six statements:

- [Statement 1/2024 on legislative developments regarding the Proposal for a Regulation laying down rules to prevent and combat child sexual abuse](#) addressed the European Commission's proposed regulation on this critical issue. While acknowledging the importance of combating such crimes, the Board emphasised the need for any measures to comply fully with fundamental rights, particularly the right to privacy and data protection. The Statement raised concerns over the potential for general and indiscriminate monitoring of private communications and called for proportionality and precision;
- [Statement 2/2024 on the financial data access and payments package](#), emphasised the critical need for comprehensive data protection mechanisms in the rapidly evolving financial technology sector, ensuring consumer trust and security;
- [Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework](#) advocated for clear delineation of duties, effective oversight powers, and adequate resources to ensure DPAs can robustly uphold data protection standards amidst increasing use of AI;
- [Statement 4/2024 on the recent legislative developments on the Draft Regulation laying down additional procedural rules for the enforcement of the GDPR](#) recommended streamlined procedures and clear guidance to facilitate swift, efficient, and

- consistent actions by regulatory authorities in the handling of cross-border cases, thus ensuring stronger protection of individuals' rights;
- [Statement 5/2024 on the Recommendations of the High Level Group on Access to Data for Effective Law Enforcement](#) responded to recommendations from the High-Level Group on data access for effective law enforcement, stressing the necessity to balance enhanced data sharing capabilities with stringent safeguards to maintain fundamental privacy protections;

- [Statement 6/2024 on the Second Report on the Application of the General Data Protection Regulation - Fostering Cross Regulatory Consistency and Cooperation](#) replied to the second European Commission report on GDPR implementation, recognising positive advancements while highlighting areas requiring further improvement.

2.4 STAKEHOLDER CONSULTATION

In 2024, the EDPB maintained its proactive engagement with stakeholders to enhance the transparency, clarity, and effectiveness of its guidelines. Committed to ensuring that guidance remains both relevant and practically applicable, the EDPB conducted targeted consultation activities throughout the year.

For the seventh consecutive year, the EDPB carried out its annual stakeholder survey under Article 71(2) GDPR, gathering critical feedback on the practical implementation of its guidelines. Key stakeholders, including data protection and privacy experts from academia, industry professionals, and representatives of non-governmental organisations, actively contributed with insights regarding the guidelines' effectiveness and usability. Respondents particularly valued the clarity and practical applicability of the guidelines, highlighting their importance in simplifying compliance tasks.

Additionally, in 2024, the EDPB organised several dedicated stakeholder events designed to foster open dialogue and mutual understanding between regulators, industry representatives, civil society organisations, and academic institutions. These interactive sessions provided stakeholders with opportunities to share experiences, discuss challenges, and propose enhancements to the regulatory framework.

Feedback from stakeholders consistently indicated the need for additional practical resources, such as visual aids, interactive materials, and explanatory content, to better clarify complex technical concepts.

To address this need, the EDPB launched a new initiative to provide concise factsheets accompanying its guidelines, aimed at meeting stakeholders' needs by simplifying and clarifying key concepts.

Overall, stakeholder consultations continued to significantly shape EDPB's initiatives, reinforcing the Board's transparency, accountability, and responsiveness.

2.5 REPRESENTING THE EDPB WORLDWIDE

In 2024, the EDPB participated in key international fora, fostering strategic collaborations, and addressing critical issues in data protection and privacy. The EDPB Chairmanship contributed to 34 high-profile speaking engagements throughout the year.

3. ENFORCEMENT COOPERATION AND ENFORCEMENT BY DPAs

Throughout 2024, national Data Protection Authorities (DPAs) continued to play a crucial role in safeguarding the data protection rights of individuals, ensuring consistent and effective enforcement of the GDPR across Europe. The EDPB facilitated coordinated actions and provided targeted support to enforcement cooperation.

3.1 EDPB ACTIVITIES TO SUPPORT GDPR ENFORCEMENT

The EDPB intensified its efforts to enhance cooperation among DPAs through targeted initiatives, launching its third coordinated enforcement action focused on the right of access, a key compliance area identified collaboratively by DPAs. Additionally, the Support Pool of Experts (SPE) reinforced DPAs' enforcement capacities, providing specialised knowledge and facilitating collaborative projects, particularly regarding intricate and emerging topics such as Artificial Intelligence, consent mechanisms in digital platforms, and facial recognition technologies.

In 2024, the EDPB signed a Memorandum of Cooperation with PEReN, an interdepartmental office operating under

the joint authority of the French Ministers of Economy, Culture, and Digital Technology. This agreement represents a significant milestone in enhancing technical collaboration to address emerging data protection challenges across Europe. Moreover, the ChatGPT taskforce was established. The taskforce emerged as a collaborative effort to bridge gaps, ensure consistent application of the GDPR, and tackle the unique risks associated with ChatGPT's processing activities.

3.2 COOPERATION UNDER THE GDPR

DPAs continued effective cooperation through the IMI system, in total, 982 procedures related to the one-stop-shop (Art. 60 GDPR) have been triggered in 2024, out of which 485 final decisions. This collaborative approach streamlined the resolution of complex cases, promoted regulatory coherence, and ensured robust protection of individual rights throughout Europe.

3.3 BINDING DECISIONS

Reflecting improved cooperation and enhanced consensus-building among DPAs, the EDPB did not adopt any binding decisions under Art. 65 GDPR and Art. 66 GDPR in 2024. The absence of such decisions underscores the effectiveness of cross-border cooperation at national level.

3.4 CASE DIGEST

In 2024, the EDPB commissioned its third thematic case digest on the right of access as part of its SPE initiative. Case digests are overviews of decisions adopted under the one-stop-shop procedure about a particular topic. The purpose of these digests is to give the DPAs and the general public, including privacy professionals, insight into decisions adopted by DPAs following cross-border cooperation procedures.

3.5 NATIONAL CASES

Throughout the year, DPAs actively exercised their corrective powers to ensure GDPR compliance across various sectors within Member States. DPAs implemented investigative measures, processing restrictions, prohibitions, and imposed substantial monetary penalties addressing significant GDPR infringements. These national enforcement actions, detailed comprehensively in the Annual Report, highlight DPAs' steadfast commitment to protecting fundamental data protection rights and promoting compliance across Europe.

In 2024, DPAs jointly issued over €1.2 billion in fines. A detailed breakdown of fines issued in 2024 can be found in Chapter 3 of the Annual Report, as well as a non-exhaustive list of national enforcement actions.

CONTACT DETAILS

Postal address

Rue Wiertz 60, B-1047 Brussels

Office address

Rue Montoyer 30, B-1000 Brussels



**EDPB-EDPS Joint Opinion
1/2022 on the Proposal
for a Regulation of the
European Parliament and of
the Council amending
Regulation (EU) 2021/953 on a
framework for the issuance,
verification and acceptance
of interoperable COVID-19
vaccination, test and recovery
certificates (EU Digital COVID
Certificate) to facilitate free
movement during the COVID-
19 pandemic**

14 March 2022

TABLE OF CONTENTS

1	Background	3
2	Scope of the opinion	4
3	COMMENTS	5
3.1	General comments.....	5
3.2	Specific comments	6
3.2.1	Lack of an evidential basis for the assessment of the necessity and proportionality of the Proposal	6
3.2.2	Modifications to current data fields.....	7

The European Data Protection Board and the European Data Protection Supervisor

Having regard to Article 42(2) of the Regulation 2018/1725 of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC,

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to the request for a Joint Opinion of the European Data Protection Supervisor and of the European Data Protection Board of 3 February 2022 regarding a Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2021/953 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic as well as regarding a Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2021/954 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) with regard to third-country nationals legally staying or residing in the territories of Member States during the COVID-19 pandemic,

HAVE ADOPTED THE FOLLOWING JOINT OPINION

1 BACKGROUND

1. On 3 February 2022, the Commission adopted a Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2021/953 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic (the "First Proposal"). The Commission proposes to base the first Proposal on Article 21(2) of the Treaty on the Functioning of the European Union (the "TFEU") according to which every EU citizen has the right to move and reside freely within the territory of the Member States¹, subject to the limitations and conditions laid down in the Treaties and by the measures adopted to give them effect.
2. On 3 February 2022, the Commission also adopted a Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2021/954 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) with regard to third-country nationals legally staying or residing in the territories of Member States during the COVID-19 pandemic amending Regulation (EU) 2021/954 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) with regard to third-country nationals legally staying or residing in the territories of Member States during the COVID-19 pandemic (the "Second

¹ References to "Member States" made throughout this document should be understood as references to "EEA Member States", and references to the "EU" should be understood as references to the "EEA".

Proposal”, and together with the First Proposal, the “Proposals”). The Commission proposes to base the Second Proposal on Article 77(2)(c) TFEU, according to which the Union shall develop policies setting out the conditions under which nationals of third countries shall have the freedom to travel within the Union.

3. The European Data Protection Board (the “EDPB”) and the European Data Protection Supervisor (the “EDPS”) note that the Proposals seek to extend the application of Regulation 2021/953 (EU Digital COVID Certificate) and, by extension, of Regulation 2021/954 by 12 months, as well as prolong for the same time the power of the Commission to adopt delegated acts pursuant to Regulation (EU) 2021/953 (the “Regulation”).
4. In addition to extending the application of the EU Digital COVID Certificate, the Proposals aim to amend certain provisions of the Regulation:
 - 1) A broadening of the definition of SARS-CoV-2 tests that rely on the detection of viral proteins (antigens) to include immunoassays performed in a laboratory setting and not only rapid antigen tests that give results in less than 30 minutes;
 - 2) An explicit clarification that vaccination certificates are to contain the number of doses administered to the holder, regardless of the Member State in which they have been administered, to make sure that the overall number actually administered is accurately reflected;
 - 3) The inclusion of vaccination certificates issued for a COVID-19 vaccine undergoing clinical trials among those certificates that may be accepted by Member States in order to waive restrictions to free movement; and
 - 4) The correction of a wrong cross-reference in Article 13(2) of Regulation (EU) 2021/953.
5. On 3 February 2022, the Commission requested a Joint Opinion of the EDPB and the EDPS on the basis of Article 42(2) of Regulation (EU) 2018/1725 (the “EUDPR”)² on the Proposals.

2 SCOPE OF THE OPINION

6. The Proposals are of particular importance due to their major impact on the protection of individuals’ rights and freedoms with regard to the processing of their personal data. The scope of this Joint Opinion is limited to the aspects of the Proposals relating to the protection of personal data, which represent a fundamental aspect of the Proposals.
7. For the sake of clarity, as the Second Proposal is limited to ensuring that Member States apply the rules laid down in the First Proposal to third country nationals who reside or stay legally in their territory and are entitled to travel to other Member States in accordance with Union law, the EDPB and the EDPS will provide their recommendations with a focus on the First Proposal. This being said,

² Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

the general comments and considerations made in this Joint Opinion are fully applicable to both Proposals.

8. Not entering into other important ethical and societal aspects on which the Proposals may have an impact in terms of compliance with fundamental rights, the EDPB and the EDPS highlight that it is essential that the Proposals are consistent and do not conflict in any manner with the application of the General Data Protection Regulation (the “GDPR”)³. This is not only for the sake of legal certainty, but also to avoid that the Proposals have the effect of directly or indirectly jeopardizing the fundamental right to the protection of personal data, as established under Article 16 TFEU and Article 8 of the Charter of Fundamental Rights of the European Union (the “Charter”).
9. The EDPB and the EDPS are aware of the ongoing legislative process of the Proposals and stress their availability to the co-legislators to provide further advice and recommendations throughout this process and to ensure in particular legal certainty for natural persons and due protection of personal data for data subjects in line with the TFEU, the Charter and EU data protection legislation.

3 COMMENTS

3.1 General comments

10. The EDPB and the EDPS recall that compliance with data protection rules does not constitute an obstacle for fighting the COVID-19 pandemic and that, at the same time, the general principles of effectiveness, necessity and proportionality must guide any measure adopted by Member States or EU institutions that involve processing of personal data to fight COVID-19⁴. A regular assessment on any measures to fight the COVID-19 pandemic should take place, having regard to the relevant scientific evidence and additional measures in place, in order to continuously evaluate which actions remain effective, necessary and proportionate. Additionally, the EDPB and EDPS also recall the principles relating to processing of personal data laid down in Article 5 of the GDPR, more specifically the principles of storage limitation, purpose limitation, as well as the principle of transparency.
11. Given the ongoing threat posed by SARS-CoV-2, including by its variant ‘Omicron’, whose increased infectiousness has resulted in very high case notification rates across the European Union and places considerable strain on healthcare systems and society; the impossibility to predict the impact of a possible increase in infections in the second half of 2022; and the risk of a prolongation of the pandemic as a result of the emergence of new SARS-CoV-2 variants, the EDPB and the EDPS understand the need to extend the applicability of the Regulation.
12. However, the EDPB and the EDPS underline that any restriction to the free movement of persons within the European Union put in place to limit the spread of SARS-CoV-2, including the requirement to present EU Digital COVID Certificates, should be lifted as soon as the epidemiological situation

³ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1.

⁴ See also EDPB Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, para. 4; EDPB’s Statement on the processing of personal data in the context of the COVID-19 outbreak. Adopted on 19 March 2020.

allows. Moreover, the EDPB and EDPS will pay special attention to the evolution of the COVID-19 pandemic and in particular to the use of personal data following the end of the pandemic.

13. The EDPB and the EDPS take note that the First Proposal does not alter substantially the existing provisions of the Regulation with regard to the processing of personal data.
14. The EDPB and the EDPS thus welcome that the GDPR will continue to apply to the processing of personal data carried out when implementing the Regulation.

3.2 Specific comments

3.2.1 Lack of an evidential basis for the assessment of the necessity and proportionality of the Proposal

15. **The EDPB and the EDPS take note that the Commission did not carry out an impact assessment for the Proposals.** According to the Commission, this is due to the urgency and the limited scope of the Proposals themselves⁵.
16. The EDPB and the EDPS recall that the original proposal for the Regulation was not accompanied by an impact assessment. In their comments made in the Joint Opinion 04/2021 on the Digital Green Certificate, the EDPB and the EDPS underlined the lack of an impact assessment accompanying the original proposal and pointed out that such an impact assessment would have provided substantiation as to the impact of the measures being adopted as well as to the effectiveness of already existing less intrusive measures⁶.
17. The EDPB and the EDPS take note of the urgency of the First Proposal, given that, in the absence of an extension of the applicability of the Regulation, the latter would cease to apply on 30 June 2022.
18. Nevertheless, also given the epidemiological developments in relation to COVID-19 in recent months, the need for an extension of the applicability of the Regulation, and by extension to Regulation 2021/954 regarding third-country nationals, could have been anticipated, and a more thorough assessment of the impact on fundamental rights, including on the right to data protection, should have been carried out.
19. In addition, the EDPB and the EDPS also highlight that, in line with Article 16 (2) of the Regulation, the Commission shall submit, by 31 March 2022, a report to the European Parliament and the Council on the application of the Regulation, containing in particular an assessment of the impact of the Regulation on the facilitation of free movement, fundamental rights and non-discrimination, as well as on the protection of personal data during the COVID-19 pandemic. **The EDPB and the EDPS strongly consider that the Proposal should be accompanied by the abovementioned report, as foreseen in the same Article of the Regulation, in order to provide a clear justification on the necessity and proportionality of the First Proposal, taking into account, amongst other things, the evolution of the epidemiological situation with regard to the COVID-19 pandemic together with the impact on**

⁵ See e.g. Explanatory Memorandum of the draft Proposal.

⁶ EDPB-EDPS Joint Opinion 04/2021 on the Proposal for a Regulation of the European Parliament and of the Council on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery to facilitate free movement during COVID-19 pandemic (Digital Green Certificate), para. 16.

fundamental rights and non-discrimination notably on the basis of the possession of a specific category of a medical certificate⁷. In addition, the EDPB and the EDPS are of the view that the report should also address other technical issues such as the security of personal data related to the use of the certificates that have arisen when applying the Regulation in practice.

20. As mentioned above, **the EDPB and the EDPS**, in this regard, **stress the need to continuously evaluate which measures remain effective, necessary and proportionate as regards the purpose of the fight against the COVID-19 pandemic**. Moreover, **the EDPB and the EDPS recall the legal imperative for the data protection principles under Article 5 GDPR to be continuously applied and integrated in any personal data processing operation**.

3.2.2 Modifications to current data fields

21. The First Proposal contains an explicit clarification that vaccination certificates are to contain the number of doses administered to the holder, regardless of the Member State in which each dose has been administered, to accurately reflect the overall number of doses administered.
22. To this end, the First Proposal seeks to amend paragraph 2, point (b) of Article 5 of the Regulation as follows [proposed changes highlighted]: “information about the COVID-19 vaccine and the number of doses administered to the holder, **regardless of the Member State in which they have been administered**”.
23. In the specific case described above, the EDPB and the EDPS understand that the proposed change seeks to address situations where individuals have received vaccination doses in different Member States. Therefore, the proposed change seems to be limited to what is strictly necessary and does not raise particular concerns from a data protection perspective.
24. This would however be different should the Commission seek to substantially modify the current data fields. In this context, **the EDPB and the EDPS recall their previous position that any modification of data fields might require a re-evaluation of the risks to fundamental rights and that only more detailed data fields (sub-categories of data) falling under the already defined categories of data should be added through the adoption of delegated acts⁸**.
25. Additionally, the EDPB and the EDPS note that the First Proposal provides that persons participating in clinical trials for the development of COVID-19 vaccines are also eligible to receive a COVID-19 vaccination certificate (EUDCC). For the sake of legal certainty, **the EDPB and the EDPS consider that the First Proposal should clarify whether the information that a data subject has participated in a clinical trial would or would not be added to the categories of data listed in Article 5(2) of the Regulation**. Should such category of data be added, the EDPB and the EDPS refer to the recommendations put forward in paragraph 41 of the EDPB-EDPS Joint Opinion 04/2021 and recalled in paragraph 23 of the current Opinion.
26. The EDPB and the EDPS further recall paragraph 39 of the Joint Opinion, in which the EDPB and the EDPS note that “*(...) an approach supporting differently comprehensive data sets and QR codes can improve data minimisation in different use cases.*” Should the Digital COVID Certificate recording the three doses, or any further possible doses, be used for purposes other than freedom of movement,

⁷ See Article 3(7) of the Regulation.

⁸ EDPB-EDPS Joint Opinion 04/2021, para. 41.

the necessary categories of personal data included in the QR code must be reassessed and different technical solutions improving data minimisation in different use cases may be needed. **The EDPB and the EDPS therefore invite the Commission to assist the Member States in developing such technical specifications⁹.**

Brussels, 14 March 2022

For the European Data Protection Supervisor

The European Data Protection Supervisor

(Wojciech Wiewiorowski)

For the European Data Protection Board

The Chair

(Andrea Jelinek)

⁹ See Formal Comments of the EDPS on the draft Commission Implementing Decision (EU) amending Implementing Decision (EU) 2021/1073 laying down technical specifications and rules for the implementation of the trust framework for the EU Digital COVID Certificate established by Regulation (EU) 2021/953 of the European Parliament and of the Council, 18 October 2021 https://edps.europa.eu/system/files/2021-10/2021-0943%20Formal_comments_EUDCC_en.pdf



**EDPB-EDPS Joint Opinion
2/2022 on the Proposal of
the European Parliament
and of the Council on
harmonised rules on fair
access to and use of data
(Data Act)**

Adopted on 4 May 2022

Executive summary

With this Joint Opinion, the EDPB and the EDPS aim to draw attention to a number of overarching concerns on the Proposal on Data Act and urge the co-legislature to take decisive action.

The EDPB and EDPS note that the Proposal would apply to a broad range of products and services, including the connected objects ('Internet of Things'), medical or health devices and virtual assistants. Certain products and services may even process special categories of personal data, such as data concerning health or biometric data. As the Proposal does not explicitly exclude certain types of data from its scope, data revealing highly sensitive information about individuals could become the object of data sharing and use according to the rules established in the Proposal.

While welcoming the efforts made to ensure that the Proposal does not affect the current data protection framework, the EDPB and the EDPS consider that additional safeguards are necessary to avoid lowering the protection of the fundamental rights to privacy and to the protection of personal data in practice. First, additional safeguards are especially necessary as the rights to access, use and share data under the Proposal would likely extend to entities other than the data subjects, including businesses, depending on the legal title under which the device is being used. Second, the EDPB and EDPS are deeply concerned by the provisions of the Proposal regarding the obligation to make data available to public sector bodies and Union institutions, agencies or bodies in case of "exceptional need". Finally, the EDPB and the EDPS are concerned that the oversight mechanism established by the Proposal may lead to fragmented and incoherent supervision.

1. The rights to access, use and share data

To limit the risks of an interpretation or implementation of the Proposal that could affect or undermine the application of existing data protection law, the EDPB and the EDPS call on the co-legislator to explicitly specify that data protection law "prevails" in case of conflict with the provisions of the Proposal insofar as the processing of personal data is concerned.

In order to promote data minimisation, products should be designed in such a way that data subjects are offered the possibility to use devices anonymously or in the least privacy intrusive way as possible, irrespective of their legal title on the device. Data holders should also limit as much as possible the amount of data leaving the device (e.g. by anonymising data).

Furthermore, the enhancement of the right to data portability mentioned in Recital 31 as one of the goals of the Proposal would require, in so far as personal data are involved, an effective empowerment of data subjects so to give them more control over their personal data. As the definition of 'user' encompasses legal persons, in case of exercise of this right by a business, this takes the form of a commercial obligation for the manufacturer/data holder to provide access to data to businesses and allow its exploitation, rather than the individuals' 'right' to access and port their personal data. In fact, according to the concept of 'user' adopted by the Proposal, individuals become entitled to enhanced portability right only incidentally, depending on the legal title under which they use the product or the related service (ownership, rental or lease) rather than on their relationship with the information concerning their private use of the product or service.

Therefore, to achieve an effective empowerment of individuals with regard to their personal data, the concept of user in Article 2(5) of the Proposal and throughout the text needs to be integrated and specified as follows: (a) adding in the definition of users "and the data subjects" (b) clearly differentiating the situations where the user is the data subject from the situation where the user is not the data subject.

Moreover, the EDPB and the EDPS recommend specifying that where the user is not the data subject, any personal data generated by the use of a product or related service shall only be made available to the user in compliance with in particular Article 6 and 9 GDPR and on the condition that, were relevant, the requirements of Article 5(3) ePrivacy Directive are fulfilled. Similar considerations apply to the making available of data to third parties upon request of a business user.

The EDPB and the EDPS stress the need to ensure that access, use, and sharing of personal data by users other than data subjects, as well as by third parties and data holders, should occur in full compliance with all of the provisions of the GDPR, EUDPR and ePrivacy Directive, including informing data subjects about the access by controllers to their personal data and facilitating the exercise of data subject rights by controllers. The EDPB and the EDPS also recall that it is important to ensure that any further processing of personal data complies in particular with Article 6(4) GDPR and, having specific regard to the possibility of automated decision-making, including profiling, with the relevant obligations provided under Article 22 GDPR.

The EDPB and the EDPS also recommend to include in the proposal clear limitations or restrictions on the use of personal data generated by the use of a product or service by any entity other than data subjects, in particular where the data at issue are likely to allow precise conclusions to be drawn concerning their private lives or would otherwise entail high risks for the rights and freedoms of the individuals concerned. In particular, the EDPS and EDPB recommend to introduce clear limitations regarding use of personal data generated by the use of a product or related services for purposes of direct marketing or advertising, employee monitoring, credit scoring or to determine eligibility to health insurance, to calculate or modify insurance premiums. This recommendation is without prejudice to any further limitations that may be appropriate, for example to protect vulnerable persons, in particular minors, or due to the particularly sensitive nature of certain categories of data (e.g. data concerning the use of a medical device or biometric data) and the protections offered by Union legislation on data protection.

2. The obligation to make data available in case of “exceptional need”

As regards Chapter V of the Proposal, the EDPB and the EDPS have deep concerns on the lawfulness, necessity and proportionality of the obligation to make data available to public sector bodies and Union institutions, agencies or bodies in case of “exceptional need”.

The EDPB and the EDPS recall that any limitation on the right to personal data must be based on a legal basis that is adequately accessible and foreseeable and formulated with sufficient precision to enable individuals to understand its scope. In accordance with the principles of necessity and proportionality, the legal basis must also define the scope and manner of the exercise of their powers by the competent authorities and be accompanied by sufficient safeguards to protect individuals against arbitrary interference.

The EDPB and the EDPS observe that the circumstances justifying the access are not narrowly specified and consider it necessary for the legislator to define much more stringently the hypotheses of emergency or exceptional need. Moreover, the EDPB and the EDPS consider certain public sector bodies and Union institutions, agencies and bodies should be excluded from the scope of Chapter V as such and should only be able to oblige data holders to make data available in accordance with the powers provided by sectoral legislation.

3. Implementation and enforcement

The EDPB and the EDPS highlight the risk of operational difficulties that might result from the designation of more than one competent authority responsible for the application and enforcement of the Proposal. The EDPB and the EDPS have serious concerns that this governance architecture will lead to complexity and confusion for both

organisations and data subjects, to divergence in regulatory approaches across the Union and thus affect consistency of monitoring and enforcement.

The EDPB and the EDPS welcome the designation of the data protection supervisory authorities as competent authorities responsible for monitoring the application of the Proposal insofar as the protection of personal data is concerned, which is important to avoid inconsistencies and possible conflicts between the provisions of the Proposal and data protection laws, and to preserve the fundamental right to the protection of personal data as established under Article 16 of the Treaty on the Functioning of the European Union (TFEU) and Article 8 of the Charter of fundamental rights of the European Union.

The EDPB and the EDPS ask the co-legislators to also designate national data protection supervisory authorities as coordinating competent authorities under this Proposal. Data protection supervisory authorities have a unique expertise, both legal and technical, in the monitoring of the compliance of data processing. Moreover, the EDPB and the EDPS are of the opinion that, considering that the GDPR applies when personal and non-personal data in a data set are inextricably linked, the role of data protection authorities should prevail in the governance architecture of the Proposal.

Having regard the oversight role of the EDPS as the data protection authority for the European Union institutions, bodies and agencies and the fact that some of the European Union institutions, bodies and agencies may also act as user or a data holder within the meaning of this Proposal, the EDPB and the EDPS recommend including a reference to the EDPS as competent authority for the supervision of the whole Proposal insofar as it concerns the Union institutions, bodies, offices and agencies.

Table of Contents

1	Background	6
2	Scope of the opinion	7
3	Assessment	7
3.1	General comments	7
3.2	Interplay of the Proposal with EU data protection laws	9
3.3	Interplay of the Proposal with DMA and DGA	11
3.4	General provisions (Chapter I of the Proposal)	12
3.4.1	Article 1: Subject matter and scope	12
3.4.2	Article 2: Definitions	12
3.5	Business to consumer and business to business data sharing (Chapter II of the Proposal)	13
3.6	Obligations for data holders legally obliged to make data available and terms related to data access and use between enterprises (Chapter III and IV of the Proposal)	17
3.7	Access to and use of data by public sector bodies and Union institutions, Agencies or Bodies (Chapter V)	20
3.8	International contexts non-personal data safeguards (Chapter VII of the Proposal)	24
3.9	Implementation and enforcement (Chapter IX of the Proposal)	24

The European Data Protection Board and the European Data Protection Supervisor

Having regard to Article 42(2) of the Regulation 2018/1725 of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC,

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

HAVE ADOPTED THE FOLLOWING JOINT OPINION

1 BACKGROUND

1. The Proposal on Data Act (“the Proposal”) is enacted pursuant to the Communication “A European Data strategy for data (“the Data Strategy”)¹.
2. The European Data Protection Board (“EDPB”) and the European Data Protection Supervisor (“EDPS”) notice that, according to the Commission “*citizens will trust and embrace data-driven innovation only if they are confident that any personal data sharing in the EU will be subject to full compliance with the EU’s strict data protection rules*”².
3. As specified in its Explanatory Memorandum, the Proposal “*is a key pillar and the second major initiative announced in the Data Strategy. In particular, it contributes to the creation of a cross-sectoral governance framework for data access and use by legislating on matters that affect relations between data economy actors, in order to provide incentives for horizontal data sharing across sectors*”. The specific objectives of the Proposal are the following:
 - “*Facilitate access to and the use of data by consumers and businesses, while preventing incentives to invest in ways of generating value through data.*
 - *Provide for the use by public sector bodies and Union institutions, agencies or bodies of data held by enterprises in certain situations where there is an exceptional data need.*
 - *Facilitate switching between cloud and edges services.*
 - *Put in place safeguards against unlawful data transfer without notification by cloud service providers.*
 - *Provide for the development of the interoperability standards for data to be reused between sectors*”³.

¹ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions “A European strategy for data”, 19 of February 2020, COM (2020) 66 final.

² A European strategy for data, Introduction, page 1.

³ Explanatory Memorandum, page 3.

2 SCOPE OF THE OPINION

4. On 23 February 2022, the Commission published the Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (“Data Act”) or (“the Proposal”).
5. On 23 February 2022, the Commission requested a Joint Opinion of the EDPB and the EDPS (“Opinion”) on the basis of Article 42(2) of Regulation (EU) 2018/1725 (EUDPR) on the Proposal.
6. **The Proposal is of particular importance for the protection of individuals’ fundamental rights and freedoms with regard to the processing of their personal data. The scope of the Opinion is limited to the aspects of the Proposal related to and involving personal data, which constitute one of the main pillars of the Proposal.**
7. The EDPB and the EDPS welcome Recital 7 of the Proposal, where it is explicitly mentioned that the Proposal complements and is without prejudice to Union law on data protection and privacy, in particular GDPR and e-Privacy Directive.
8. The EDPB and the EDPS highlight that **it is necessary to ensure and uphold the respect and the application of the EU acquis in the field of personal data protection. When personal data are involved in the context of the Proposal, it is essential to clearly avoid in the legal text of the Proposal any inconsistency and possible conflict with the GDPR, e-Privacy Directive or EUDPR.** This not only for the sake of legal certainty, but also to avoid that the Proposal has the effect of directly or indirectly jeopardizing the fundamental rights to privacy and the protection of personal data, as established under Articles 7 and 8 of the Charter of fundamental rights of the European Union (the “Charter”) and Article 16 of the Treaty on the Functioning of the European Union (“TFEU”).
9. Since the Proposal, as further explained in this Opinion, raises several concerns regarding the protection of the fundamental rights to privacy and the protection of personal data, **the aim of this Opinion is not to provide an exhaustive list of all the issues, nor always to provide alternative proposals of wording suggestions.** Instead, **this Opinion aims at addressing the main criticalities, with respect to privacy and data protection, of the Proposal.**

3 ASSESSMENT

3.1 General comments

10. The EDPB and the EDPS acknowledge the goal to unleash the potential of information to be extracted from data in order to gain valuable knowledge for important common values and for health, science, research and climate action. In addition, they highlight that the GDPR already allows for this as far as personal data are concerned.
11. The EDPB and the EDPS also acknowledge the importance of and welcomes the aim of providing a more effective right to data portability, with a view of facilitating innovation and promoting competition and to empower consumers using products or related services to meaningfully control how the data generated by their use of the product or related service are used⁴.

⁴ Explanatory Memorandum, p. 13.

12. The Proposal aims to lay down harmonised rules on making data generated by the use of a product or related service available to the user of that product or service and on the making data available by data holders to data recipients⁵. The EDPB and EDPS therefore recognise that the envisaged scope of application of the Proposal does not exclusively concern personal data, but instead would apply to both personal and non-personal data that are generated by the use of products or services within the meaning of the Proposal.
13. The EDPB and the EDPS note, however, that the enhanced right to portability would extend to **a broad range of products and services that may reveal highly sensitive data** concerning individuals, including children and other vulnerable categories of data subjects. The Proposal explicitly targets data generated by the IoT and IoB, including vehicles, home equipment and consumer goods, medical and health devices.⁶ The data generated by these connected objects will become subject matter of the data access rights and obligations introduced by the Proposal. As a result, data from the most private places and surroundings of data subject may be processed, as well as highly sensitive health data.
14. The Proposal does not distinguish between personal data, as defined under Article 4(1) of the GDPR, and other non-personal data in defining the scope of the rights of access, sharing and use of data. Moreover, **the rights to access, use and share data under the Proposal would in practice likely extend to entities other than the data subject**, including businesses, depending on the legal title under which the product is used. The data sharing rights and obligations that the Proposal intends to set up therefore create a **substantial risk of personal data being collected, shared and used without knowledge of the data subject**, notably if not specified according to the recommendations made in this Opinion, in particular in case of exercise of the right to data portability by a user other than the data subject. Illustrations of problematic use cases include, without being limited to, devices tracking the location of products or services carried or operated by data subjects which are not “users” in the sense of the Proposal.
15. The EDPB and the EDPS are concerned that the Proposal in its current text would extensively push a development towards “commodification” of personal data, whereby personal data are seen as a mere tradeable commodity. This would not only undermine the very concept of human dignity and the human-centric approach the EU wants to uphold in its Data Strategy, but it would also risk undermining the rights to privacy and data protection as fundamental rights⁷.
16. The EDPB and the EDPS acknowledge and welcome the efforts made to ensure that the Proposal does not affect the current data protection regime provided by the GDPR and the ePrivacy Directive. That being said, the EDPB and the EDPS consider that **additional safeguards are necessary** to avoid lowering the protection of the fundamental rights to privacy and to the protection of personal data in practice.
17. In the remainder of this Opinion, the EDPB and the EDPS provide recommendations on how to make the relevant data protection principles, safeguards and obligations more effective within the Proposal. Given the wide scope of the rights and obligations set out in the Proposal with regard to data access, use and sharing, general references to the GDPR are not sufficient. The EDPB and the EDPS consider further specifications necessary, in particular where the text of the Proposal risks giving rise to misinterpretation if a more complete reference to data protection law (both GDPR and ePrivacy

⁵ Article 1(1) of the Proposal.

⁶ Recital (14) of the Proposal.

⁷ See in this regard also https://edpb.europa.eu/system/files/2021-05/edpb_statementondga_19052021_en_0.pdf p. 4.

Directive) is not explicitly highlighted. The EDPB and the EDPS consider that, absent such specifications, there is a risk that the Proposal lowers the level of protection for data subjects, contrary to the stated objectives of Commission.

18. These recommendations are also due to the unclear scope (referring to non-personal and/or to personal data) of the rights and obligations to access to, share and use data by data holders, users (as non-data subjects) and third parties or recipients laid down in the Proposal.
19. Therefore, the EDPB and the EDPS remark that, considering that the enhanced right to portability would extend to a broad range of products and services that may reveal highly sensitive data concerning individuals, in order not to undermine the level of protection of personal data, the Proposal should expressly and clearly specify that processing of personal data by data holders, users (as non-data subjects) and third parties or recipients shall be subject to all conditions and rules provided by data protection legislation⁸.

3.2 Interplay of the Proposal with EU data protection laws

20. The EDPB and the EDPS note that Article 1(3) of the Proposal specifies that “Union law on the protection of personal data, privacy and confidentiality of communications and integrity of terminal equipment shall apply to personal data processed in connection with the rights and obligations laid down in this Regulation”, and that the Proposal “shall not affect the applicability of Union law on the protection of personal data, in particular Regulation (EU) 2016/679 and Directive 2002/58/EC, including the powers and competences of supervisory authorities.” Moreover, the same provision establishes that “[i]nsofar as the rights laid down in Chapter II of this Regulation are concerned, and where users are the data subjects of personal data subject to the rights and obligations under that Chapter, the provisions of this Regulation shall complement the right of data portability under Article 20 of Regulation (EU) 2016/679.”
21. The EDPB and the EDPS very much welcome the objective of Article 1(3) of the Proposal, which is to ensure that the application of existing data protection rules and principles shall not be affected or undermined. In its Statement on the Digital Services Package and Data Strategy⁹, the EDPB called upon the Commission to ensure legal certainty and coherence with the existing data protection framework. In particular, the EDPB encouraged the Commission to ensure that data protection rules and principles shall prevail whenever personal data are being processed.
22. The EDPB and the EDPS positively note that the compromise text of the Data Governance Act (“the DGA”), both in its recitals and enacting terms, explicitly state that in the event of conflict between the provisions of the DGA and Union law or national law on the protection of personal data adopted in accordance with Union law, the latter should prevail¹⁰.
23. The EDPB and the EDPS strongly recommend amending Article 1(3) of the Proposal to align it with the wording of the DGA in order to enhance coherence between the Proposal, the DGA and the existing

⁸ See in particular paragraph 22, and footnote 8, of the Opinion.

⁹ EDPB Statement on the Digital Services Package and Data Strategy, 18 November 2021.

¹⁰ Article 1(2a) and Recital 3a of the Draft regulation on European data governance (Data Governance Act) - text subject to revision, December 2021, available at <https://www.consilium.europa.eu/en/press/press-releases/2021/11/30/promoting-data-sharing-presidency-reaches-deal-with-parliament-on-data-governance-act/>

legislation on the protection of personal data. The EDPB and the EDPS consider that a reference to Regulation (EU) 2018/1725 EUDPR should be introduced in Article 1(3) and in Recital 30¹¹.

24. The EDPB and the EDPS consider this explicit statement necessary in light of the entities which may benefit from the right to access, use and share data generated by the use of products or related service. The Proposal assigns these rights to the ‘user’, who is defined as ‘*a natural or legal person that owns, rents or leases a product or receives a [service]*’¹². Recital 18 clarifies that a user might be a *business or consumer* who has purchased, rented or leased the product. As result, the right to access, use and share data in practice is likely to extend to entities other than the data subject, including businesses, depending on the legal title under which the product is used¹³.
25. The EDPB and the EDPS recognise that entities other than the data subject may have a legitimate reason to access data generated by the use of a product or related service. At the same time, the EDPB and the EDPS consider that there is also a significant risk that the rights to access, share or use data generated by the use of a product or related service could be exercised to unduly interfere with the rights and freedoms of data subjects. For example, an employer that has purchased virtual voice assistants and made them available to its employees could use the right to access in order to access their search history.
26. To limit the risks of an interpretation or implementation of the Proposal that could affect or undermine the application of existing data protection law, the EDPB and the EDPS call on the legislator to strengthen the wording of Article 1(3) by explicitly specifying that, in case of conflict with the provisions of the Proposal data protection law “**prevails**”, insofar as it concerns the processing of personal data.
27. Finally, the EDPB and the EDPS also recommend to **clearly distinguish** in Article(s) 3, 4, 5, 6, 8 of the Proposal between the rights of data subjects to access and use data generated by their own use of products or related services and the possible rights or obligations of other actors. Access and sharing of personal data **by users other than the data subject** should **only be possible** insofar as all applicable data protection principles and rules allow such processing of personal data¹⁴.
28. For example, the EDPB and the EDPS would welcome a Recital stating that, in accordance with the GDPR, the performance of a contract can only be a legal ground for processing of personal data if the data subject is a party or if steps are being taken at the request of the data subject prior to entering into a contract. Furthermore, this Recital should also mention that the requirement of ‘necessity’ is not satisfied by the mere inclusion of a contractual clause providing for the processing. The controller should be able to demonstrate how the main subject-matter of the specific contract with the data

¹¹ While Article 1(2)d of the Proposal indicates that this Regulation applies to “*public sector bodies and Union institutions, agencies or bodies that request data holders to make data available where there is an exceptional need to that data for the performance of a task carried out in the public interest and the data holders that provide those data in response to such request*” (i.e. EUIs making requests pursuant Chapter V), it does not exclude EUIs from the notion of “user” nor of the notion of “recipient”. In any event, any request emanating from a EUI should also comply with the EUDPR (in addition to the requirements set forth in Chapter V).

¹² Article 2(5) of the Proposal refers to ‘a services’, but should be corrected to refer to the singular ‘service’.

¹³ See also Recital 18 of the Proposal.

Insofar as it concerns personal data, the nature of the enhanced right to data portability needs to be clarified: in case of exercise of this right by a business, this would be about the commercial obligation for the manufacturer/data holder to provide access to data to business, subject to all conditions and limits of the GDPR, rather than a ‘right’ to port and have processed personal data.

subject cannot, as a matter of fact, be performed if the specific processing of the personal data in question does not occur¹⁵.

3.3 Interplay of the Proposal with DMA and DGA

29. The EDPB and the EDPS note that the Proposal aims at **complementing**¹⁶ the Proposal for a **Digital Markets Act** ('DMA')¹⁷ and the DGA¹⁸.
30. The EDPB and the EDPS observe that **undertakings designated as gatekeepers under the DMA** shall not be eligible **third parties** for the data sharing pursuant to the Proposal¹⁹.
31. The EDPB and the EDPS note that the Proposal **does not clarify the interplay with some key provision of the DMA** related to data sharing, notably with Article 6(1)(h)²⁰ and Article 6(1)(i)²¹ of the DMA. In this regard, the EDPB and the EDPS recommend aligning the Proposal to the final text of the DMA agreed by the co-legislators.
32. The EDPB and the EDPS consider in particular that certain constraints on **types of data to be made available**, for instance query, click and view data (from online searches) referred to in Article 6(1)(j) of the DMA, to be made available in anonymised form²², should also apply, *mutatis mutandis*, in the context of data sharing related to queries made to virtual assistants.
33. Having regard to the DGA, the EDPB and the EDPS remark that the Proposal includes a **different definition** than the one found in the in the DGA for the term 'data holder'²³, which may create legal uncertainty. Moreover, the definition of "data holder" in the Proposal should be further clarified²⁴.
34. The EDPB and the EDPS consider that the enacting terms of the Proposal should further clarify if, and subject to which conditions, a 'data recipient'²⁵ can be a '**provider of data sharing services**'²⁶ (or 'data intermediation service'²⁷) as referred to in the DGA. Recital 35 refers to the case where the third party

¹⁵ EDPB 2/2019 Guidelines on the processing of personal data under Article 6(1)(b) GDPR on the context of the provision of online services to data subjects Version 2.0, adopted on 8 October 2019.

¹⁶ Explanatory Memorandum of the Proposal, pages 4 and 5.

¹⁷ COM(2020)842 final.

¹⁸ [COM\(2020\) 767 final](#).

¹⁹ Article 5(2) of the Proposal.

The EDPB and the EDPS also note the exclusion from the scope of the enhanced right to data portability of data generated by the use of products or related services provided by micro or small enterprises pursuant to Article 7(1).

²⁰ Article 6(1)(h) of the DMA Proposal, which would require gatekeepers among others to provide tools for end-users to facilitate the exercise of data portability, in line with GDPR, including by the provision of continuous and real-time access Note: at the moment of drafting, 1/4/2022, there is not yet any publicly available copy of the compromise text (contrary to the DGA).

²¹ Article 6(1)(i) of the DMA Proposal which would require gatekeepers to provide continuous and real-time access to and use of aggregated or non-aggregated only where directly connected with the use effectuated by the end-user in respect of the products or services offered by the relevant business user through the relevant core platform service, and when the end-user opts in to such sharing with a consent in the sense of the GDPR.

²² See also EDPS Opinion 2/2021 on the Proposal for a Digital Markets Act, 10 February 2021, paragraph 32, page 12, "*the gatekeeper shall be able to demonstrate that anonymised query, click and view data have been adequately tested against possible re-identification risks.*"

²³ The Proposal contains a definition of 'data holder' under Article 2(6); the Proposal for the DGA under Article 2(5).

²⁴ The meaning of "*through control of the technical design of the product and related services*" might need to be specified.

²⁵ As defined under Article 2(7) of the Proposal.

²⁶ '*data intermediation service providers*' in the Council compromise text, LIMITE, 10 December 2021 [to be checked, updated once/if a public version is available]

²⁷ See Article 9 of the Proposal for a Data Governance Act (DGA).

is a provider of a data intermediation service within the meaning of the DGA, and further specifies that in this case the safeguards for the data subject provided for by the DGA apply. However, the substance of Recital 35 of the Proposal is not mirrored by a provision in the enacting terms of the Proposal. The EDPB and the EDPS recommend specifying the specific safeguards for data subjects contained in the DGA that would be applicable to the data sharing from data holders to third parties as intermediaries pursuant to the Proposal. Moreover, in line with the remarks made in section 3.2, the Proposal should specify that these safeguards complement the ones laid down in the GDPR, as well as in the e-Privacy Directive²⁸, and notably in accordance with this Directive, the requirement of consent of the end-user to the data processing by the third party.

3.4 General provisions (Chapter I of the Proposal)

3.4.1 Article 1: Subject matter and scope

35. The EDPB and the EDPS note that, due to the use of very broad concepts, such as ‘product’ and ‘related services’ in Article 1(1) of the Proposal, the scope is also very broad and could benefit from more clarity²⁹.
36. Article 1 (4) of the Proposal states that it shall not affect Union and national legal acts providing for the sharing, access and use of data for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including Regulation (EU) 2021/784 and the [e-evidence proposals [COM(2018) 225 and 226] nor shall it affect the respective provisions of Directive(EU) 2015/849 and of the Regulation (EU) 2015/847. Finally, the competences of the Member States regarding activities concerning public security, defence, national security, customs and tax administration and the health and safety of citizens in accordance with Union law are not either affected by the proposal.
37. It is however unclear if Article 1 (4) of the Proposal has any relevant interplay with these Regulations and this Directive. To state that the Proposal does not affect these laws does not mean that data processing operations under the Proposal cannot be used for the purposes of these laws. The EDPB and EDPS recommend to further specify the possible interplays with the abovementioned legal frameworks³⁰.

3.4.2 Article 2: Definitions

38. The definition of ‘data’ under Article 2(1) of the Proposal could, depending on the nature of the data at hand, also include personal data, implying that rules in the Proposal may apply next to the GDPR. The term data is used in the Proposal indistinctively to refer to personal and non-personal data, which may lead to confusion. For instance, the reference in Recital 24 to the possibility for data holders to use data generated by the user on the basis of a contractual agreement does not clarify which type of data it refers to. If this example refers also to personal data, it is incomplete with regard to the obligations that controllers have pursuant to the GDPR, and could therefore be easily misinterpreted.

²⁸ ePrivacy Directive: Art. 5(3).

²⁹ See WP29 opinion 8/2014 on the recent developments on the internet of things, adopted on 16 September 2014.

³⁰ See also section 3.7 of the Opinion Regarding access to and use of data by public sector bodies and Union institutions, agencies or bodies pursuant to Chapter V of the Proposal.

39. The EDPB and EDPS therefore recommend the co-legislator to supplement Article 2 of the Proposal with a definition of ‘personal data’ (as defined by GDPR) and ‘non personal data’. In a similar fashion, the EDPB and EDPS recommend to add definitions of ‘data subject’ and ‘consent’ into Article 2 of the Proposal, as these terms are frequently used in the Proposal and the recitals. Article 2 (5) of the Proposal defines ‘user’ as a natural or legal person that owns, rents or leases a product or receives a service. For the sake of clarity and to achieve an effective empowerment of individuals with regard to their personal data, the EDPB and EDPS recommend to add to this definition “and the data subject” (and to include a definition of data subject as having the same meaning as in the GDPR) as well as to clearly differentiate the situations where the user is the data subject from the situation where the user is not the data subject.

3.5 Business to consumer and business to business data sharing (Chapter II of the Proposal)

40. Chapter II of the Proposal relates to data generated by the use of products or related services. The Proposal defines a “product” as “*a tangible, movable item [...] that obtains, generates or collects, data concerning its use or environment, and that is able to communicate data via a publicly available electronic communications service and whose primary function is not the storing and processing of data*”. A ‘related service’, in turn, is defined as “*a digital service, including software, which is incorporated in or inter-connected with a product in such a way that its absence would prevent the product from performing one of its functions*”. Moreover, the Proposal clarifies in Article 7(2) that where the Proposal refers to products or related services, such reference shall also be understood to include virtual assistants³¹, insofar as they are used to access or control a product or related service.
41. The EDPB and the EDPS consider that the definition of product overlaps, in part, with the **notion of “terminal equipment”**³² **within the meaning of Article 5(3) ePrivacy Directive**. Article 5(3) of the ePrivacy Directive requires consent of the subscriber or user prior to the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or end-user, unless such storage or access is strictly necessary in order for the provider of an information society service to provide the service explicitly requested by the subscriber or user. Moreover, any processing operations of personal data following these processing operations, including processing personal data obtained by accessing information in the terminal equipment, must also have a legal basis under Article 6 GDPR in order to be lawful³³.

³¹ Article 2(4) provides the definition of virtual assistant.

³² According to Article 1(1)(a) of Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment, “terminal equipment” includes “*equipment directly or indirectly connected to the interface of a public telecommunications network to send, process or receive information; [...]*”.

See also EDPB Guidelines 02/2021 on virtual voice assistants, Version 2.0, adopted on 7 July 2021, para. 25: “*In accordance with the definition of “terminal equipment”, smartphones, smart TVs and similar IoT devices are examples for terminal equipment. Even if VVAs in themselves are a software services, they always operate through a physical device such as a smart speaker or a smart TV. VVAs use electronic communications networks to access these physical devices that constitute “terminal equipment” in the sense of the e-Privacy Directive. Consequently, the provisions of Article 5 (3) e-Privacy Directive apply whenever VVA stores or accesses information in the physical device linked to it*”.

³³ See EDPB Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications, paragraph 41 for similar reasoning regarding connected vehicles (“EDPB Guidelines 1/2020”). See also EDPB, Opinion 5/2019 on the interplay between the e-Privacy Directive and the GDPR, in particular regarding to competence, tasks and powers of data protection authorities.

42. The EDPB and the EDPS positively note the clarification provided by Recital 15 of the Proposal, which clearly indicates that products such as personal computers, servers, tablets and smart phones, cameras, webcams, sound recording systems and text scanners would not be covered by the Proposal. That being said, the EDPB and the EDPS consider that Article 2(2) of the Proposal defines a “product” in such (broad) terms that such devices might in fact fall within the scope of the definition included in the enacting terms of the Proposal. The EDPB and the EDPS therefore consider it necessary to amend the definition of “product” so as to clearly exclude products such as personal computers, servers, tablets and smart phones, cameras, webcams, sound recording systems and text scanners, also in the enacting terms of the Proposal³⁴.
43. The EDPB and the EDPS positively note that Article 4(5) of the Proposal lays down that where the user is not a data subject, any personal data generated by the use of a product or related service shall only be made available by the data holder to the user where there is a valid legal basis under Article 6(1) of Regulation (EU) 2016/679 and, where relevant, the conditions of Article 9 of Regulation (EU) 2016/679 are fulfilled. As the Proposal assigns the right to access and use data generated by the use of products or related services to “users” (which encompasses entities other than data subjects), the EDPB and the EDPS consider that such clarification constitutes an important safeguard. As the lawfulness of processing of personal data is governed by Article 6 GDPR as a whole, however, **the EDPB and the EDPS recommend to replace the reference to Article 6(1) GDPR in Article 4(5) of the Proposal by a reference to Article 6 GDPR as a whole and more in general to all rules conditions provided by data protection legislation.** Moreover, as access to data generated by the use of products or related services may also involve access to information stored on the terminal equipment of a subscriber or user, the EDPB and the EDPS recommend clarifying that data shall only be made available by the data holder to the user on the condition that, were relevant, the conditions of **Article 5(3) ePrivacy Directive** are fulfilled.
44. The EDPB and the EDPS recall that where consent is required pursuant to Article 5(3) ePrivacy Directive, consent under Article 6 GDPR would be most probably the adequate legal basis in relation to any processing of personal data following the storing of information, or gaining access to, information already stored in the terminal equipment of a subscriber or user³⁵.
45. Similar considerations apply to the making available of data to third parties upon request of a business user under Article 5(6) of the Proposal. In addition, the EDPB and the EDPS recommend to further align the wording of Article 5(6) with Article 4(5) of the Proposal, by stipulating that data generated by the use of a product or related service shall only be made available “by the data holder to the third party” where all conditions and rules provided by data protection legislation are complied with, notably where there is a valid legal basis under Article 6 and where relevant, the conditions of Article 9 the GDPR and Article 5(3) of the ePrivacy Directive are fulfilled.
46. As a result, the EDPB and the EDPS stress the need to ensure that **access, use, and sharing of personal data by users other than data subjects should occur in full compliance with all the GDPR and ePrivacy obligations**, including informing data subjects about the access by controllers to their personal data and facilitating the exercise of data subject rights by controllers.

³⁴ The EDPB and EDPS wish to underline that the finding that the definition of “product” in the Proposal overlaps, in part, with the definition of “terminal equipment” within the meaning of Article 5(3) of the ePrivacy Directive, should not be understood as recommendation to revise the definition of “product” to align it with the definition of “terminal equipment”.

³⁵ See EDPB Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications, paragraph 27.

47. Having regard, in particular, to **Article 3(1)** and 4(1) of the Proposal, the EDPB and the EDPS consider that, in order to promote **data minimisation**, products should be designed in such a way that **the data subjects** (irrespective of their legal title on the device) are offered the possibility **to use the products covered by the Proposal, in particular Internet of Bodies (“IoB”) or Internet of Things (“IoT”)** devices **anonymously** or in the least privacy intrusive way as possible. Data holders should also limit as much as possible the amount of data leaving the device (e.g. by anonymising data).³⁶ The Proposal should clearly specify this aspect in order to strengthen control by the data subjects on their personal data. **Article 3(2)(a)** of the Proposal, referring to the obligation to provide information to the user on the nature and volume of data likely to be generated by the use of the product, should not be interpreted as adversely affecting the GDPR data minimisation principle. Finally, the EDPB and the EDPS note that Article 3 should clearly indicate which entity/ entities shall be required to comply with the obligations listed in Article 3(1) and Article 3(2) of the Proposal. In the interest of legal certainty, the EDPB and EDPS recommend to indicate clearly which entity/entities shall be responsible for each of the obligations listed.
48. The EDPB and the EDPS note that **the limitation on keeping records** on business access to data under **Article 4(2)** and on third parties' access to data under **Article 5(3)** of the Proposal should not be interpreted as adversely affecting the GDPR obligations on security of personal data and on accountability. These provisions should clearly specify this important aspect.
49. The EDPB and the EDPS also note that, pursuant to **Article 5(9)³⁷** of the Proposal, the right of the user to share data with third parties “shall **not affect data protection rights of others**”. In this regard, the EDPB and the EDPS stress the need to clarify **the scope** and the meaning of this provision. Furthermore, in order to ensure **consistency** with the right of the data subjects under Article 20 GDPR that the Proposal aims at complementing, the EDPB and the EDPS recommend referring in a Recital to the criteria for **balancing** the right to portability **with data protection concerns related to other persons** laid down in the EDPB guidelines on data portability³⁸.
50. **Article 6** of the Proposal specifies that third parties shall process data made available to them pursuant to Article 5 only for the purposes and the conditions agreed with the user, and subject to the rights of the data subject insofar as personal data are concerned, and shall delete the data when they are no longer necessary for the agreed purpose. Moreover, Article 6(2)(b) provides that the third party shall not use, data for profiling of data subjects, unless it is necessary to provide the service requested by the user. Having regard to the scenario of the user being an entity other than the data subject, the EDPB and the EDPS recall that it is important to ensure that **any further processing of personal data complies with Article 6(4) GDPR and, having specific regard to the profiling scenario, with the relevant obligations provided under, with Article 22 of the GDPR, where applicable**. In case of processing of special categories of personal data (e.g. such as data concerning health or sex life), explicit consent by the data subject will in principle be required, unless another exception to the prohibition contained in Article 9 GDPR can be invoked. Where Article 5(3) of the ePrivacy Directive applies, the data should only be processed with the consent of the subscriber or user, unless strictly

³⁶ See WP29 opinion 8/2014 on the recent developments on the internet of things, adopted on 16 September 2014.

³⁷ Article 4 of the Proposal should contain a similar provision having regard to Article 4(1).

³⁸ See WP29 (endorsed by EDPB) Guidelines on the right to data portability, at pages 11-12.

necessary in order to provide an information society service explicitly requested by the subscriber or user³⁹.

51. For the sake of legal certainty, and to avoid a possible interpretation according to which the relevant data protection rules in the context of the obligations to process personal data by third parties pursuant to Article 6(1) of the Proposal are only the ones referring to data subjects' rights (Chapter III of the GDPR), as also recommended in paragraphs 43 and 45 of the Opinion, the EDPB and the EDPS recommend complementing the wording in Article 6(1) referring to the GDPR "and subject to the rights of the data subject insofar as personal data are concerned", replacing it by the following: "and where all conditions and rules provided by data protection legislation are complied with, notably where there is a valid legal basis under Article 6 and where relevant, the conditions of Article 9 of the GDPR and Article 5(3) of ePrivacy Directive are fulfilled and subject to the rights of the data subject insofar as personal data are concerned."
52. Concerning Article 6(2)(a), the EDPB and the EDPS welcome the prohibition for the third party to coerce, deceive or manipulate the user in any way.⁴⁰ The EDPB and EDPS also welcome the reference to so-called 'dark patterns' in Recital 34 of the Proposal. The EDPB and EDPS note, however, that the factors that might affect decision-making may be different depending on whether or not the user is also the data subject. **The EDPB and EDPS therefore recommend making explicit that Article 6(2)(a) of the Proposal prohibits any form of coercion, deception, or manipulation of data subjects** (regardless of whether the user is also the data subject).
53. Similar considerations apply in relation to Article 6(2)(b) of the Proposal: the third party should not be allowed to use the data it receives for profiling of natural persons unless it is necessary to provide the service requested by the data subject. In addition, the EDPB and the EDPS consider that "the service" to be provided by the third party as requested by the user (which may be an entity other than the data subject) is not defined in the Proposal. It is therefore possible that such 'services' could entail a serious interference with the rights and freedoms of individuals or otherwise have a significant impact on the persons concerned.
54. Therefore EDPB and the EDPS recommend to include in the proposal clear limitations or restrictions on the use of personal data generated by the use of a product or service by any entity other than the data subject (either as "user", "data holder" or "third party"), in particular where the data at issue is likely to allow precise conclusions to be drawn concerning their private lives or would otherwise entail high risks for the rights and freedoms of the individuals concerned.
55. In particular, the EDPS and EDPB recommend to introduce limitations regarding use of personal data generated by the use of a product or related services for purposes of direct marketing or advertising, employee monitoring, credit scoring or to determine eligibility to health insurance, to calculate or modify insurance premiums. This recommendation is without prejudice to any further limitations that may be appropriate, for example to protect vulnerable persons, in particular minors, or due to the particularly sensitive nature of certain categories of data (e.g. data concerning the use of a medical device) and the protections offered by Union legislation on data protection.

³⁹ See also EDPB guidelines on processing personal data in the context of connected vehicles and mobility related applications, Version 2.0, adopted on 9 March 2021, paragraph 15.

⁴⁰ As specified by Recital 34, referring to so-called 'dark patterns'.

56. Moreover, the EDPB and the EDPS recall as a general principle that also third party as a controller is subject to the principle of data minimisation and that anonymisation techniques shall be used whenever possible. Compliance with the data minimisation principle is particularly important in the case of data capable of revealing intimate aspects of an individual's private life⁴¹.

3.6 Obligations for data holders legally obliged to make data available and terms related to data access and use between enterprises (Chapter III and IV of the Proposal)

57. Chapter III addresses the conditions, including compensation, under which data shall be made available where a data holder is obliged to make data available to a data recipient as in Chapter II or in other Union law or Member State legislation.
58. In this regard, Article 8 of the Proposal foresees no role for, or reference to the data subject as terms and conditions for data sharing have to be determined in an agreement between the data holder and the data recipient. Indeed, in cases where the user is an entity other than the data subject, the latter is not part of the contract under the Proposal. This risks to severely compromise the effectiveness of data protection rights. Further risks in this context may stem from intermediation services and data brokerage, which could relate data that originally may be considered non-personal to specific data subjects⁴².
59. In any case, the EDPB and the EDPS stress that the right to the protection of personal data enshrined in Article 16(1) TFEU and in Article 8 of the Charter, as a right related to each natural person, is inalienable and cannot be waived by any agreement between the data holder and the data recipient⁴³.
60. Pursuant to Article 8(3) of the Proposal the data holder shall not discriminate between "comparable categories of data recipients" and, as per Article 8(4) of the Proposal, the data holder cannot make data available to a data recipient on an exclusive basis. These obligations however should not undermine the right of informational self-determination of data subjects according to which they are entitled to discriminate among the recipients of their personal data (notably, when they consent to the processing, for instance in case the conditions of Article 5(3) of the ePrivacy Directive are applicable or the processing relies on consent under Article 6 GDPR). Therefore, the EDPB and the EDPS call for a wording which effectively enhances data holders' and data recipients' compliance with the GDPR. In particular, the EDPB and the EDPS recommend that the clarification provided in Recital 41 according to which these obligations are without prejudice to the GDPR is included in the text itself of Article 8.
61. Pursuant to Article 9 of the Proposal, any compensation required by the data holder to third parties has to be reasonable, and for SMEs it cannot exceed the costs incurred for making the data available, unless otherwise specified in sectoral legislations.

⁴¹ See EDPB statement on the Digital Services Package and Data Strategy, adopted on 18 November 2021, stressing "*the importance of the obligation of data protection by design and by default, which is particularly relevant in the context of 'connected objects' (e.g. the Internet of Things and the Internet of Bodies), due to the significant risks to the fundamental rights and freedoms of the persons concerned.*"

⁴² The more non-personal data are combined with other available information, the more the re-identification risk for data subjects increases. See EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act), page 16.

⁴³ See the EDPB Statement on the Digital Services Package and Data Strategy adopted on 18 November 2021, page 6.

62. Regarding Article 9 of the Proposal on the compensation for making data available, the EDPB and the EDPS strongly recommend to waive any ambiguity concerning the monetary transactions accompanying the sharing of personal data. According to Recital 42 of the proposal, the right to require compensation for making data available to third parties "*should not be understood as paying for the data itself but in the case of micro, small or medium-sized enterprises, for the costs incurred and investment required for making the data available*". This statement, however, read in conjunction with Recital 46 seems to imply that, on the contrary, in the case of data sharing between large companies, or when the data holder is a small or medium-sized enterprise and the data recipient is a large company the right for data holder to set 'reasonable compensation' to be met by third parties, may be considered as an incentive to monetise personal data.
63. In this respect, the EDPB and the EDPS reiterate that data protection is a fundamental right guaranteed by Article 8 of the Charter and personal data cannot be considered as a tradeable commodity.
64. In cases where parties disagree on the terms and conditions of making data available, the Proposal envisages alternative ways of resolving disputes that may arise between data holders and data recipients. According to Article 10 of the Proposal, these parties can seek the assistance of dispute settlement bodies certified by the Member States. However, where personal data are made available to third parties upon a request of users **who are not the data subjects**, the latter would be completely excluded from the participation to dispute settlement proceedings concerning the sharing of their personal data between the data holder and the data recipient. In addition, given the complex interactions and overlaps between the data subject's rights under the GDPR and the rights and obligation established by the Proposal, it should be taken into consideration that the parties' decision to submit a dispute to a dispute settlement body may interfere with the data subject's right to lodge a complaint with a supervisory authority.
65. More in general, the EDPB and the EDPS strongly recommend stating clearly that the dispute settlement under Article 10 shall not encroach upon data subject's rights and controllers' processor obligations established under the GDPR. In addition, paragraphs 5 and 9 of Article 10 must be amended so as to take into account that data subjects shall not be prevented from their right to seek redress before a supervisory authority.
66. The Proposal also encourages the application by the data holder of appropriate technical protection measures, including smart contracts, to prevent unauthorised access to the data and to ensure compliance with the rights and obligations arising from the proposal as well as with the agreed contractual terms for making data available (Article 11). In this regard, it should be clarified how smart contracts can constitute the means to provide data holders and data recipients with adequate guarantees that the transmitted data is prevented from unauthorised disclosure or access and that the agreed terms and conditions for sharing this data are fulfilled. In order to ensure consistency with Article 32 of the GDPR, the EDPS and the EDPB underline that to the extent that personal data is involved, paragraph 1 of Article 11 must include a reference to the obligation of implementing appropriate technical and organisational measures so as to ensure a level of security appropriate to the risk of the personal data processing.
67. Concerning Article 11(2) the EDPB and the EDPS recommend stating clearly that, insofar as it concerns personal data, the data holder's authorisation to share data cannot replace the requirement of an appropriate legal basis according to the GDPR or alternatively specifying that this authorisation applies in case of processing of non-personal data. Moreover, the same paragraph has to be amended in order to establish that any instruction from the data holder or the user (who is not necessarily the data

subject) to destroy the data made available to the data recipients and any copies thereof must not be of prejudice to the data subject's right to restriction of processing under Article 18 of the GDPR.

68. With regard to the exceptions envisaged by paragraph 3 of Article 11, the Proposal should clarify how and by whom the situations described under letter a) and b) can be judged applicable. In addition, these exceptions must take into account not only the harm to and the interests of the data holder but also and primarily the harm to the data subjects as well as their rights and interests with regard to their rights to privacy and data protection. Therefore, the EDPB and the EDPS recommend to add in Article 11 a new paragraph explicitly stating that paragraph 2(b) shall apply in case of possible harm to data subjects or prejudice to their rights and interests.
69. Finally, the reference in Article 12(1) to the data holder's obligation, under Article 5 of the Proposal, to make data available upon a user's request, suggests that as far as personal data is concerned, and despite what's said in Recital 24 when the user is an entity other than the data subject⁴⁴, the Proposal could be interpreted as creating a legal basis under Article 6(1)(c) of the GDPR for the sharing of personal data. Therefore, appropriate, specific and effective safeguards for the protection of the rights and interests of data subjects as far as personal data are concerned should be added especially where the user is not the data subject. Consequently, given the complex interactions and overlaps between the data subject's rights under the GDPR and the rights and obligation established by the Proposal, Article 12(2) of the proposal should be amended in order to specify that any contractual term in a data sharing agreement between data holders and data recipients which, to the detriment of the data subjects, undermines the application of their rights to privacy and data protection, derogates from it, or varies its effect, shall not be binding on that party.
70. In Chapter IV, Article 13 of the Proposal, the EDPB and the EDPS highlight that the Proposal state that "*a contractual term is unfair if it is of such a nature that its use grossly deviates from good commercial practice in data access and use, contrary to good faith and fair dealing.*" Similarly to what is mentioned above, regarding the consistency of the definitions with the GDPR, this provision is not clear enough given the fact that the concept of personal data or non-personal data or mixed data sets is not clear throughout the text.
71. Data access and use constitute processing of personal data pursuant to Article 4(2) of the GDPR. Therefore, when personal data are involved in the processing, the obligations of the GDPR for controllers and processors shall apply. The same applies to the cases where mixed data sets (i.e. both personal and non-personal data) are involved.
72. To this purpose, the EDPB and the EDPS urge the co-legislature to clarify in the Proposal the relevant requirements and obligations of controllers and processors where personal data are processed, in the manner specified in this Opinion⁴⁵.

⁴⁴ Recital 5 of the Proposal when it states that the latter "should not be interpreted as recognising or creating **any legal basis for the data holder to hold, have access to process (personal) data...**" seems to be in contraction with Article 5 of the Proposal establishing the data holder's obligation to make data available upon a user's request, since according to the definition under Article 4(2) GDPR, the 'processing' of personal data encompasses any operation or set of operations performed on personal data or on sets of personal data, including "disclosure by transmission, dissemination or otherwise making available...".. However, if Recital 5 concerns the data processing by the data holder for its own purposes, this should be clarified.

⁴⁵ See in particular at paragraphs 39-39 and 67 of this Opinion. See also at paragraphs 43, 45, 46 and 51 of this Opinion.

3.7 Access to and use of data by public sector bodies and Union institutions, Agencies or Bodies (Chapter V)

73. As regards the ‘making data available’ to public sector bodies and Union institutions, agencies or bodies (‘public sector bodies’) based on ‘exceptional need’ (Chapter V of the Proposal), the EDPB and the EDPS have serious concerns on the **lawfulness, necessity and proportionality** of the obligation to make data available to public sector bodies and Union institutions, agencies or bodies.
74. Article 14 of the Proposal provides that, upon request, a data holder (exception made for SMEs) shall make data available to a public sector body or to Union institution, agency or body **demonstrating an exceptional need to use the data requested**. The Proposal does not refer to legislative measures to be adopted to provide the legal basis for this obligation. The EDPB and the EDPS note that Article 1(2)(d) of the Proposal refers to a task carried in the public interest.⁴⁶ In the same vein, Article 15(c) of the Proposal refers to a task carried in the public interest “*that has been explicitly provided by law*”. This suggests that the Proposal envisages Article 6(1)(c) GDPR as a lawful basis for the processing carried out by the relevant public sector body, Union institution, agency or body. The EDPB and the EDPS note, however, that neither the relevant tasks of public interest, nor the public sector bodies, Union institutions, agencies or bodies who have been tasked with these missions of public interest have been clearly identified by the Proposal. Instead, the Proposal sets out a number of conditions that would give rise to a legal obligation for the data holder to provide personal data.
75. Article 17(1)(d) of the Proposal provides that, when requesting data pursuant to Article 14(1), the public sector body or Union institution, agency or body shall state in the request **the legal basis for requesting the data**. In the interest of legal certainty, the EDPB and the EDPS consider that Article 17(1)(d) should specify that the request shall clearly indicate the legal provision that explicitly assigns the task of public interest to the public sector body, Union institution, agency or body making the request.
76. Article 15 of the Proposal specifies three possible alternative scenarios where the exceptional need to use data is deemed to exist. As for cases (a) and (b) of Article 15 of the Proposal, the EDPB and the EDPS consider that the requirement “*explicitly provided by law*” should be explicitly included, since any limitation on the right to personal data must be “*provided for by law*” (Article 52(1) of the Charter, as confirmed by consolidated case law of the CJEU).
77. Limitations must be based on a legal basis that is adequately **accessible and foreseeable** and formulated with **sufficient precision to enable individuals to understand its scope**. In accordance with the principles of necessity and proportionality, the legal basis must also define the **scope and manner** of the exercise of the power by the competent authorities and be accompanied by **sufficient safeguards** to protect individuals against arbitrary interference⁴⁷.
78. Against this background, the EDPB and the EDPS observe in the first place that the **circumstances** justifying the access are not narrowly specified. The Proposal refers to “**exceptional need**”, which would justify the request of data, relating to a “**public emergency**” (which is broadly defined⁴⁸). The EDPB and the EDPS note that Recital 57 specifies that the existence of a public emergency is

⁴⁶ See also Recital (5) of the Proposal.

⁴⁷ See, among others, CJEU, C-175/20, “SS” SIA v. Valsts ienēmumu dienests, ECLI:EU:C:2022:124, para. 83.

⁴⁸ Article 2(10) defines a ‘public emergency’ as “*an exceptional situation negatively affecting the population of the Union, a Member State or part of it, with a risk of serious and lasting repercussions on living conditions or economic stability, or the substantial degradation of economic assets in the Union or the relevant Member State(s)*”

determined according to the respective procedures in the Member States or of relevant international organisations. The EDPB and the EDPS recommend including this important specification in the operative part of the Proposal. In addition, the EDPS and EDPB consider it **necessary for the legislator to define much more stringently the hypotheses of emergency or exceptional need**. The definition of “public emergency” contained in Article 2(10) of the Proposal should therefore be amended to more clearly delineate the types of situations that would constitute a public emergency.

79. The scenario under letter (c) of Article 15 of the Proposal is actually presenting two very different use cases: a first one in which access to the data would be granted to fulfil a public interest; a second one in which access to the data would be granted to reduce administrative burden. With regard to the first use case, referring to the lack of available data prevents the public sector body from fulfilling a specific task in the public interest is **particularly problematic** having regard to the requirement of ‘quality of law’ (including foreseeability) providing for interferences with fundamental rights. As for the second use case, the **mere reduction of the administrative burden can difficultly outweigh the impact on the fundamental rights and freedoms of the persons concerned**. At the same time, it would not fulfil the requirement of the necessity of the interference on fundamental rights and freedoms. In this regard, the EDPB and the EDPS advocate in particular a more explicit delimitation of the circumstances in which the request can be made.
80. The EDPB and EDPS note that the **categories of personal data** to be accessed by public sector bodies are not sufficiently specified⁴⁹. However, the obligation to provide data could extend to personal data from devices forming the IoT⁵⁰ and the IoB. Such information could concern special categories of personal data and other sensitive data such as location that would enable to draw intimate inferences on the data subject’s life.
81. The EDPB and the EDPS also note that the **safeguards for data subjects** are not adequately spelled out in the Proposal. In particular, Article 17(2)(c) of the Proposal (which concerns **the content of the requests** for data by the public authority) refers to respect for the legitimate aims of the data holder, but not to the risks for the rights and freedoms *of the data subject*. According to Article 19(1)(b) of the Proposal, the public sector body *having received data* shall implement, technical and organisational measures that safeguard the rights and freedoms of the data subjects. In this regard, the EDPB and the EDPS stress that the aforesaid measures shall be taken first and foremost *at the moment of the collection* of data, rather than following data transmission.
82. Article 17(2)(d) of the Proposal specifies that the request shall concern, insofar as possible, *non-personal* data. This safeguard is accompanied by the provision under Article 18(5), according to which where compliance with the request requires disclosure of personal data, the data holder shall take reasonable efforts to pseudonymise the data, insofar as the request can be fulfilled with pseudonymised data. The EDPB and the EDPS consider that Article 18(5) should be amended so that the data holder is required to pseudonymise the data, not just “to take reasonable efforts”. Therefore, the EDPB and the EDPS call the co-legislator to delete the reference to “to take reasonable efforts” since this reference seems to limit the data holder’s obligation and recall that. Pseudonymisation mitigates risks for the data subjects by reducing the amount of personal data processed and the impact of an eventual data breach. In addition, the EDPB and the EDPS recommend the co-legislator to take into account that other appropriate safeguards according to the GDPR may need to be

⁴⁹ Recital 56 refers to “data held by an enterprise”.

⁵⁰ Recital 14.

implemented by the data holder, notably adequate technical and organizational measures ensuring minimization, integrity and confidentiality of personal data.

83. More broadly, the EDPB and the EDPS observe that the public sector body enjoys a **broad discretion** when requesting data pursuant to the Proposal, since it is its request (and not the Proposal itself) that specifies among others: what data are required (Article 17(1)(a)); the ‘exceptional need’ (letter (b)), which only in case of public emergency is determined according to established procedures; the purpose of the request, as well as the intended use and the duration ‘of the use’ (letter c)).
84. The EDPB and the EDPS consider that the Proposal should more **clearly define the scope and manner of the exercise of the power by the public sector body** to protect individuals against arbitrary interference⁵¹. In particular, the EDPB and the EDPS recall that, according to case law of the CJEU⁵², the legislation providing the legal basis for the measures at stake must lay down clear and precise rules governing **the scope and application** of the measure in question and imposing **minimum safeguards**, so that the persons whose personal data is affected have **sufficient guarantees** that data will be effectively protected against the risk of abuse. That legislation must indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where the protection of the special categories of personal data is at stake.
85. Moreover, the EDPB and the EDPS note that according to Article 17(3) of the Proposal, public sector bodies shall **not make data available for reuse within the meaning of Directive (EU) 2019/1024**. Article 17(4), however, would allow the exchange of data between public sector bodies in the pursuit of the tasks referred to in Article 15 or the sharing of data with third parties in cases of outsourcing of ‘technical inspections or other functions’ by public sector bodies. Given the broad scope of Article 15, the limitation on reuse of data, including personal data, is not defined in a sufficiently narrow way. Moreover, Recital 65 of the Proposal specifies that “*Data made available to public sector bodies and to Union institutions, agencies and bodies on the basis of exceptional need should only be used for the purpose for which they were requested, unless the data holder that made the data available has expressly agreed for the data to be used for other purposes.*” The EDPB and EDPS recall that insofar as the request concerns personal data, any processing for a purpose other than that for which the personal data have been collected would be governed by Article 6(4) GDPR and/or Article 6 EUDPR, notwithstanding any expression of agreement by the data holder. Therefore, the EDPB and EDPS recommend amending the said provisions accordingly.
86. **Article 21** of the Proposal would allow further transmission of the data by public sector bodies **to natural or legal persons in view of carrying out research related to the purpose for which data was requested**. The EDPB and the EDPS recall the need for **appropriate safeguards**, taking into account

⁵¹ See in this regard, EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, 19 December 2019, referring among others to the following safeguards: the notification to the person affected; the provision for the data to be retained in the European Union; the provision for the irreversible destruction of the data at the end of the retention period. See also CJEU, C-175/20, “*SS” SIA v. Valsts ienēmumu dienests*”, ECLI:EU:C:2022:124, para. 64, but also para. 83 and 84.

⁵² See CJEU, C-623/17, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs*, ECLI:EU:C:2020:790, para. 68.

the potentially sensitive nature of the data at issue, in accordance with Article 89 GDPR and Article 13 EUDPR.

87. The EDPB and the EDPS also recall, as indicated in the EDPB Statement on the Digital Services Package and Data Strategy, that "*particular attention should be paid to the safeguards for processing for the purposes of scientific research, ensuring lawful, responsible and ethical data management, such as vetting requirements for researchers who will have access to large amounts of potentially sensitive personal data*"⁵³. The EDPB and the EDPS recommend integrating these requirements in the Proposal.
88. Concerning Article 18 of the Proposal, the EDPB and the EDPS consider that the reference to "sectoral legislation" (defining specific needs on the availability of data under Article 18(2)) should be specified. A specific remark concerns Article 18(6), establishing the competence of the authority referred to in Article 31 in case, among others, of challenges against the execution of the request. Since the requesting authority can be an EU Institution, agency or body, Article 31 should include the EDPS and a reference to Regulation (EU) 2018/1725. A reference should also be included in this provision to the notification of the request to the data subject and to the possibility for the data subject (not only for the data holder) to challenge the request, as well to her or his right to an effective judicial remedy against the request.
89. Concerning Article 19 of the Proposal, the EDPB and the EDPS observe that the broad definition of purposes also dilutes the safeguard under Article 19(1)(a). Moreover, the data retention period applicable depending on the purpose of the data processing should be clearly defined from the outset.
90. Article 16(2) of the Proposal specifies that "the rights from this Chapter *shall not be exercised* by public sector bodies *in order to carry out* activities for the prevention, investigation, detection or prosecution of criminal or administrative offences or the execution of criminal penalties, or for customs or taxation administration. "This Chapter *does not affect* the applicable Union and national law on the prevention, investigation, detection or prosecution of criminal or administrative offences or the execution of criminal or administrative penalties, or for customs or taxation administration (emphasis added).
91. As a preliminary remark, the EDPB and the EDPS note that the provision in Article 16(2) is not aligned with Article 1(4), which specifies that the Proposal, in all its provisions, shall not affect a number of data processing activities and of competences that partially differ from the ones identified in Article 16(2). Moreover, the EDPB and the EDPS note that Recital 60 of the Proposal already confirms that public sector bodies and Union institutions, agencies and bodies should *rely on their powers under sectoral legislation* for the exercise of their tasks in the areas of prevention, investigation, detection or prosecution of criminal and administrative offences, the execution of criminal and administrative penalties, as well as the collection of data for taxation or customs purposes.
92. Given the specific nature and mission of public sector bodies and Union institutions, agencies and bodies that carry out such tasks of public interest, however, the EDPB and the EDPS consider that such entities should be excluded from the scope of Chapter V as such. Indeed, the EDPB and the EDPS consider that such entities should *only* be able to oblige data holders to make data available in accordance with the powers provided exclusively by sectoral legislation. Moreover, in particular as regards Union institutions, agencies and bodies, the EDPB and the EDPS recommend explicitly

⁵³ EDPB Statement on the Digital Services Package and Data Strategy, adopted on 18 November 2021, page 7.

identifying those entities that would be able to request data in accordance with Chapter V, having due regard to the their competences as set out in their founding acts, in the enacting terms of the Proposal.

93. These recommendations are without prejudice to the need to sufficiently specify the overly broad definition of 'public emergency' in Article 2(10) that would justify the exercise of the power of access to data.

3.8 International contexts non-personal data safeguards (Chapter VII of the Proposal)

94. The EDPB and the EDPS welcome the provisions of the Proposal relating to data access which are limited to only non-personal data and seem to mirror the provisions of Article 48 of the GDPR. The EDPB and the EDPS note that in substance Article 27 primarily concerns access requests rather than transfers. The notion of "transfer" has a specific meaning under the GDPR that entails obligations to frame them. In order to avoid any confusion with respect to non-personal data, the EDPB and the EDPS suggest to refer only to access and remove the notion of transfer from this article.
95. In addition, a clarification would be useful as to the interplay between the Article 27(1) and Article 27(2) and 27(3) of the Proposal. The EDPB and the EDPS welcome the statement in article 27(1) which covers any risk of governmental access to non-personal data that would create a conflict with Union law or the national law of the relevant Member State. However, the final wording of provision, "*without prejudice to paragraph 2 or 3*" should be revised to make clear that even if there is no request, the measures provided in paragraph 1 have to be put in place in any case, i.e. irrespective of any request for access to data by a third country. Indeed, as the information regarding a request is not always available, it is important to put in place the measure to avoid such possibility of access. The EDPB and the EDPS also question whether the word "reasonable" in paragraph 1 does not reduce the impact of the measures. The EDPB and the EDPS would suggest to remove the word "reasonable" in order to ensure the efficiency of such measures or replace it by a more compelling term such as "necessary".
96. Moreover, the EDPB and the EDPS note that according to Article 27(3) of the Proposal, providers of data processing services receiving a decision to transfer or give access to non-personal data held in the Union by a court or an administrative authority of a third country may ask the opinion of competent authorities or bodies pursuant to the Proposal in order to determine whether the applicable access conditions are met. The EDPB and the EDPS welcome this provision requiring the consultation of the competent authority in specific cases. However, the consequences of the opinion of the competent authority are not specified in the provision. The EDPB and the EDPS therefore suggest to add that "*If the opinion of the competent authorities concludes that the conditions are not met, in particular because the decision concerns commercially sensitive data or affects the interests of the Union or its Member States in matters of national security or defence, then the recipient shall not provide access to the data*".

3.9 Implementation and enforcement (Chapter IX of the Proposal)

97. As a general comment regarding the provisions on governance of this Regulation, the EDPB and the EDPS would like to underline the risks posed by the Proposal which does not harmonize the supervision of the application of this Regulation between Member States, does not provide for a European consistency mechanism that could ensure the consistent application of this Regulation within the internal market, nor provides harmonized penalties, thus risking forum shopping.

98. Article 31 of the Proposal provides that each Member State shall designate one or more competent authorities as responsible for the application and enforcement of the Data Act, and that Member States may establish one or more new authorities or rely on existing authorities. The EDPB and the EDPS highlight the risk of operational difficulties that might result from the designation of more than one competent authority responsible for the application and enforcement of this Regulation. The EDPB and the EDPS have serious concerns that this draft governance architecture will lead to complexity and confusion for both organisations and data subjects, divergence in regulatory approaches across the Union and thus affect the consistency in terms of monitoring and enforcement.
99. Regarding the sectoral authorities, the provision of Article 31(2)(b) is quite vague and does not give sufficient guidance regarding the allocation of responsibilities between competent authorities, data protection authorities and sectoral authorities related to the implementation of the Proposal, thus raising a risk of overlapping and conflict of attribution. For example, the precise role of national authorities responsible for the enforcement of consumer protection (mentioned in Recital 82 and Articles 36 and 37 of this Regulation) is not defined in Chapter IX of the Proposal. The powers and tasks of the different competent authorities should be clearly defined, notably regarding the enforcement of the different provisions of the Proposal. As an example, the EDPB and the EDPS recommend that the co-legislators determine which authority shall be responsible for the application and enforcement of Chapter IV of the Proposal on unfair terms related to data access and use between enterprises. Moreover, the interplay between the governance model of the Proposal and those provided by sectoral legislations (e.g. with the competent authorities established by the Health Data Space Regulation) should be made clearer and more detailed in order to ensure legal certainty and avoid confusion.
100. The EDPB and the EDPS welcome the designation of data protection supervisory authorities as competent authorities responsible for monitoring the application of the Proposal insofar as the protection of personal data is concerned (Article 31(2)(a)). This designation is important to avoid inconsistency and possible conflict between the provisions of this Regulation and the GDPR, and to preserve the fundamental right to the protection of personal data as established under Article 16 TFEU and Article 8 of the Charter. However, the competence of the supervisory authorities is "*without prejudice to paragraph 1*". It is unclear how such provision could affect the competence of data protection supervisory authorities and sectoral authorities. Therefore, the EDPB and the EDPS call the co-legislator to modify this provision so to remove any ambiguity.
101. Moreover, it is unclear how Article 31(1) interacts with Article 31(4) of the Proposal. The Proposal provides many scenarios, which lack clarity. The EDPB and the EDPS consider that the Proposal as currently drafted could lead to conflicts of attribution, complexity for organisations and data subjects, as well as fragmented supervision between Member States. Therefore, for the sake of clarity, the EDPB and the EDPS recommend the deletion of the reference to "*without prejudice to paragraph 1 of this Article*" (Article 31(2)). The EDPB and the EDPS also strongly recommend the co-legislators to clarify Article 31(1) and 31(4) and set out clear provisions on the designation of competent, data protection, sectoral and coordinating authorities, on the attribution of responsibilities between these authorities and cooperation mechanism. Notably, the EDPB and the EDPS flag the absence of defined powers and tasks of the coordinating competent authority in the Proposal, and recommend that the co-legislator rectify that.
102. Article 31(3) of the Proposal lays down the obligation of Member States to ensure that the respective tasks and powers of the competent authorities designated pursuant to paragraph 1 of said Article are clearly defined. The EDPB and the EDPS note that many of these powers and tasks are similar with

those attributed to data protection supervisory authorities according to Article 58 of the GDPR. Nevertheless, the EDPB and the EDPS consider that Article 31(3) of the Proposal does not harmonize tasks and powers of competent authorities among Member States and the interplay between this provision and the GDPR is not clear. Furthermore, it is unclear how these tasks and powers listed in Article 31(3) of the Proposal will affect the tasks and powers exercised by the data protection supervisory authorities when monitoring the application of this Regulation insofar as the protection of personal data is concerned. It could be understood from Article 31(2)(a) that the tasks and powers of data protection supervisory authorities shall be those established by Chapter VI and VII of the GDPR. However, it is unclear whether new tasks and powers are to be assigned to these authorities by the Proposal, and if this is the case how the latter will interact with the tasks and powers assigned to the data protection supervisory authorities by the GDPR. To ensure clarity and consistency of the monitoring, the EDPB and the EDPS recommend to clearly define the envisaged role of data protection supervisory authorities in the context of the Proposal.

103. The EDPB and the EDPS welcome Article 31(6) of the Proposal, which establishes that competent authorities shall remain free from any external influence and shall neither seek nor take instructions from any other entity. In order to clarify and strengthen this provision, the EDPB and the EDPS recommend to explicitly mention the independent nature of competent authorities in the Proposal.
104. According to Article 32(1) of the Proposal, without prejudice to any other administrative or judicial remedy, natural and legal persons shall have the right to lodge a complaint, individually or, where relevant, collectively, with the relevant competent authority in the Member State of their habitual residence, place of work or establishment if they consider that their rights under this Regulation have been infringed.
105. The right to lodge a complaint pursuant to Article 32 may raise operational difficulties as it is unclear how natural or legal persons will determine if personal data are concerned and which authority is competent to handle their complaint. The EDPB and the EDPS strongly recommend that the legislator provide a clear and precise cooperation mechanism for the handling of complaints between competent authorities (i.e. data protection supervisory authorities, sectoral authorities and coordinating authorities), and establishes a clear port of entry for complainants. The EDPB and the EDPS consider that Articles 32(2) and 32(3) are insufficient, and do not provide enough information neither for complainants nor for supervisory authorities. The EDPB and the EDPS recommend that the coordinating authorities be designated as point of entry for all complaints related to this Regulation, with the task to distribute it to relevant other authorities. The EDPB and the EDPS notably recommend to explicitly mention that Chapter VIII of the GDPR is not affected by this Article.
106. It is also unclear how this Provision will interact with the one-stop-shop mechanism provided by Article 56 of the GDPR for cross-border processing as far as personal data are concerned.
107. Furthermore, the EDPB and the EDPS note the absence of specific provisions on the right to effective judicial remedy by any affected natural or legal person with regard to a failure to act on a complaint lodged with competent authorities, as well as with regard to decisions of competent authorities under this Proposal. This might lead to parallel and inconsistent regimes between the enforcement under the GDPR (for which a right to effective judicial remedy is provided) and the Proposal.
108. The EDPB and the EDPS note that Recital 82, Articles 36 and 37 of the Proposal establish the possibility to make use of the EU consumer protection cooperation network mechanism and to enable representative actions by amending the Annexes to the Regulation (EU) 2017/2394 and Directive (EU)

2020/1828. It is unclear how and to what extent the consumer protection cooperation network mechanism will interact with this Article right to lodge a complaint.

109. With regard to Article 33, the EDPB and EDPS note that the Proposal does not harmonize the penalties for infringements of the Proposal (nor specifies the violations that shall be sanctioned, the fines for the infringements of its provisions, nor the authorities or bodies competent to apply such penalties). For example, it is unclear how and which authority will be responsible for the enforcement of Article 5(2) which prohibits gatekeepers from acting as a third party with whom a user can share its data, and what penalties will be applicable. The EDPB and the EDPS recommend that the co-legislator clarifies the interplay between the Proposal and the DMA regarding the enforcement of this provision and the penalties applicable.
110. The EDPB and the EDPS notice that this provision, limiting the enforceability of the Proposal (the capability to impose harmonised sanctions), and possibly also giving raise to forum-shopping for the most lenient Member State, is prejudicial to the stated aim of the Proposal to ensure fairness in the allocation of value from data among actors in the data economy.
111. With regard to Article 34, the EDPB and the EDPS recommend that the Commission shall consult the European Data Protection Board when developing and recommending non-binding model contractual terms on data access and use, as far as personal data as concerned.
112. Finally, the EDPB and the EDPS note the absence of a European cooperation framework in the Proposal. Considering the impact of the Proposal across Member States, and the high quantity of cross-border processing that might fall under the scope of this Regulation, it is quite surprising that this Proposal does not provide a clear European cooperation mechanism in order to ensure its consistent application among Member States (especially with respect to the handling of complaints and taking into account the possible involvement of different sectoral competent authorities). The EDPB and the EDPS note that Article 31(3)(f) of the Proposal is insufficient in this sense and recommend the co-legislator to establish clear rules in order to facilitate the cooperation between the different authorities involved.
113. The EDPB and the EDPS welcome the designation of national data protection authorities as competent authorities responsible for monitoring the application of the Proposal insofar as the protection of personal data is concerned, and ask the co-legislators to also designate national data protection authorities as coordinating competent authorities under this Proposal.
114. Data protection authorities have a unique expertise, both legal and technical, in the monitoring of the compliance of data processing, in providing guidance to digital players and data subjects, and in the use of inter-regulation mechanism, placing them at the core of the digital regulation landscape.
115. Moreover, the EDPB and the EDPS are of the opinion that, considering that the GDPR applies when personal and non-personal data in a data set are inextricably linked, the role of data protection authorities should prevail in the governance architecture of this Proposal. The co-legislators should make sure that this governance reflects the prevalence of the fundamental right to the protection of personal data established under Article 16 TFEU and Article 8 of the Charter, and preserves the independence of data protection authorities.
116. The designation of coordinating competent authorities other than data protection authorities could affect consistency in terms of monitoring the application of the provisions of the GDPR and lead to real complexity for digital players and data subjects.

117. The EDPB and the EDPS note that the EDPS is only mentioned in Article 33(4) of the Proposal, which refers to penalties (for infringements of provision on public bodies' access to data, Chapter V) and is not listed as a "competent authority" in Article 31 of the Proposal. Having regard the EDPS **oversight role** as the data protection authority for the European Union institutions, bodies and agencies and the fact that some of the European Union institutions, bodies and agencies may also act as user or a data holder within the meaning of this Proposal, the EDPB and the EDPS recommend including **a reference to the EDPS as competent authority in Article 31(2)(a) for the supervision of the whole Proposal insofar as it concerns the Union institutions, bodies, offices and agencies.** Moreover, it should be clarified that, where relevant, Article 62 of Regulation 2018/1725 shall apply *mutatis mutandis*.

Brussels, 4 May 2022

For the European Data Protection Board

The Chair

(Andrea Jelinek)

For the European Data Protection Supervisor

The European Data Protection Supervisor

(Wojciech Wiewiorowski)

Adopted



EDPB-EDPS
Joint Opinion 5/2021
on the proposal for a
Regulation of the European
Parliament and of the Council
laying down harmonised rules
on artificial intelligence
(Artificial Intelligence Act)

18 June 2021

Executive Summary

On 21 April 2021, the European Commission presented its Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (hereinafter “the Proposal”). The EDPB and the EDPS welcome the concern of the legislator in addressing the use of artificial intelligence (AI) within the European Union (EU) and stress that the Proposal has prominently important **data protection implications**.

The EDPB and the EDPS note that the **legal basis** for the proposal is in the first place Article 114 of the Treaty on the Functioning of the European Union (TFEU). In addition, the Proposal is also based on Article 16 of the TFEU insofar as it contains specific rules on the protection of individuals with regard to the processing of personal data, notably restrictions of the use of AI systems for ‘real-time’ remote biometric identification in publicly accessible spaces for the purpose of law enforcement. The EDPB and EDPS recall that, in line with the jurisprudence of the Court of Justice of the EU (CJEU), Article 16 TFEU provides an appropriate legal basis in cases where the protection of personal data is one of the essential aims or components of the rules adopted by the EU legislature. The application of Article 16 TFEU also entails the **need to ensure independent oversight for compliance** with the requirements regarding the processing of personal data, as is also required Article 8 of the Charter of the Fundamental Rights of the EU.

Regarding the **scope of the Proposal**, the EDPB and EDPS strongly welcome the fact that it extends to the provision and use of AI systems by EU institutions, bodies or agencies. However, the **exclusion of international law enforcement cooperation from the scope** set of the Proposal raises serious concerns for the EDPB and EDPS, as such exclusion creates a significant risk of circumvention (e.g., third countries or international organisations operating high-risk applications relied on by public authorities in the EU).

The EDPB and the EDPS **welcome the risk-based approach** underpinning the Proposal. However, this approach should be clarified and the concept of “risk to fundamental rights” aligned with the GDPR and the Regulation (EU) 2018/1725 (EUDPR), since aspects related to the protection of personal data come into play.

The EDPB and the EDPS agree with the Proposal when it states that the classification of an **AI system as high-risk does not necessarily mean that it is lawful** per se and can be deployed by the user as such. **Further requirements resulting from the EU data protection law may need to be complied with** by the controller. Moreover, the compliance with legal obligations arising from Union legislation (including on personal data protection) should be a precondition to being allowed to enter the European market as CE marked product. To this end, the EDPB and the EDPS consider that **the requirement to ensure compliance with the GDPR and EUDPR should be included in Chapter 2 of Title III**. In addition, the EDPB and the EDPS consider necessary to adapt the conformity assessment procedure of the Proposal so that third parties always conduct high-risk AI systems’ *ex-ante* conformity assessments.

Given the great risk of discrimination, the Proposal prohibits “social scoring” when performed ‘over a certain period of time’ or ‘by public authorities or on their behalf’. However, private companies, such as social media and cloud service providers, also can process vast amounts of personal data and conduct social scoring. Consequently, **the future AI Regulation should prohibit any type of social scoring**.

Remote biometric identification of individuals in publicly accessible spaces poses a high-risk of intrusion into individuals’ private lives, with severe effects on the populations’ expectation of being anonymous in public spaces. For these reasons, the EDPB and the EDPS **call for a general ban on any use of AI for an automated recognition of human features in publicly accessible spaces** - such as of faces but also of

gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals - in any context. A **ban** is equally recommended **on AI systems categorizing individuals from biometrics into clusters** according to ethnicity, gender, as well as political or sexual orientation, or other grounds for discrimination under Article 21 of the Charter. Furthermore, the EDPB and the EDPS consider that the use of AI to **infer emotions of a natural person is highly undesirable and should be prohibited.**

The EDPB and the EDPS welcome the **designation of the EDPS as the competent authority and the market surveillance authority for the supervision of the Union institutions, agencies and bodies.** However, the role and tasks of the EDPS should be further clarified, specifically when it comes to its role as market surveillance authority. Furthermore, the future AI Regulation should clearly establish the **independency of the supervisory authorities** in the performance of their supervision and enforcement tasks.

The designation of data protection authorities (DPAs) as the national supervisory authorities would ensure a more harmonized regulatory approach, and contribute to the consistent interpretation of data processing provisions and avoid contradictions in its enforcement among Member States. Consequently, the EDPB and the EDPS consider that **data protection authorities should be designated as national supervisory authorities pursuant to Article 59 of the Proposal.**

The Proposal assigns a predominant role to the Commission in the “European Artificial Intelligence Board” (EAIB). Such role conflicts with the need for an AI European body to be independent from any political influence. To ensure its independency, the future AI Regulation should give **more autonomy to the EAIB** and ensure it can act on its own initiative.

Considering the spread of AI systems across the single market and the likelihood of cross-border cases, there is a crucial need for a harmonized enforcement and a proper allocation of competence between national supervisory authorities. The EDPB and EDPS suggest envisaging **a mechanism guaranteeing a single point of contact for individuals concerned by the legislation as well as for companies, for each AI system.**

Concerning the **sandboxes**, the EDPB and the EDPS **recommend clarifying their scope and objectives.** The Proposal should also clearly state that the legal basis of such sandboxes should comply with the requirements established in the existing data protection framework.

The **certification system** outlined in the Proposal is **missing a clear relation to the EU data protection law** as well as to other EU and Member States’ law applicable to each ‘area’ of high-risk AI system and is not taking into account the **principles of data minimization and data protection by design** as one of the aspects to take into consideration **before obtaining the CE marking.** Therefore, the EDPB and the EDPS recommend amending the Proposal as to clarify the relationship between certificates issued under the said Regulation and data protection certifications, seals and marks. Lastly, the DPAs should be involved in the preparation and establishment of harmonized standards and common specifications.

Regarding the **codes of conduct**, the EDPB and the EDPS consider it **necessary to clarify** if the protection of personal data is to be considered among “additional requirements” that can be addressed by these codes of conduct, and to ensure that the “technical specifications and solutions” do not conflict with the rules and principles of the existing EU data protection framework.

TABLE OF CONTENTS

1	INTRODUCTION	5
2	ANALYSIS OF THE KEY PRINCIPLES OF THE PROPOSAL	7
2.1	Scope of the Proposal and relationship with the existing legal framework	7
2.2	Risk-based approach	8
2.3	Prohibited uses of AI.....	10
2.4	High-risk AI systems.....	12
2.4.1	Need for an <i>ex-ante</i> conformity assessment by external third parties	12
2.4.2	Scope of regulation must also cover AI systems already in use	13
2.5	Governance and European AI Board	13
2.5.1	Governance	13
2.5.2	The European AI Board	15
3	INTERACTION WITH THE DATA PROTECTION FRAMEWORK	16
3.1	Relationship of the Proposal to the existing EU data protection law	16
3.2	Sandbox & further processing (Articles 53 and 54 of the Proposal)	17
3.3	Transparency	19
3.4	Processing of special categories of data & data relating to criminal offences	19
3.5	Compliance mechanisms.....	20
3.5.1	Certification	20
3.5.2	Codes of conduct.....	20
4	CONCLUSION	22

The European Data Protection Board and the European Data Protection Supervisor

Having regard to Article 42(2) of the Regulation (EU) 2018/1725 of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC¹,

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018²,

Having regard to the request for a Joint Opinion of the European Data Protection Supervisor and of the European Data Protection Board of 22 April 2021 regarding the proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act),

HAVE ADOPTED THE FOLLOWING JOINT OPINION

1 INTRODUCTION

1. The advent of artificial intelligence ('AI') systems is a very important step in the evolution of technologies and in the way humans interact with them. AI is a set of key technologies that will profoundly alter our daily lives, be it on a societal or an economic standpoint. In the next few years, decisive decisions are expected for AI as it helps us overcome some of the biggest challenges we face in many areas today, ranging from health to mobility, or from public administration to education.
2. However, these promised advances do not come without risks. Indeed, the risks are very relevant considering that the individual and societal effects of AI systems are, to a large extent, unexperienced. Generating content, making predictions or taking a decision in an automated way, as AI systems do, by means of machine learning techniques or logic and probabilistic inference rules, is not the same as humans carrying out those activities, by means of creative or theoretical reasoning, bearing full responsibility for the consequences.
3. AI will enlarge the amount of predictions that can be done in many fields starting from measurable correlations between data, invisible to human eyes but visible to machines, making our lives easier and solving a great number of problems, but at the same time will erode our capability to give a causal interpretation to outcomes, in such a way that the notions of transparency, human control, accountability and liability over results will be severely challenged.
4. Data (personal and non-personal) in AI are in many cases the key premise for autonomous decisions, which will inevitably affect individuals' lives at various levels. This is why the

¹ OJ L 295, 21.11.2018, p. 39–98.

² References to "Member States" made throughout this document should be understood as references to "EEA Member States".

EDPB and the EDPS, already at this stage, strongly assert that the Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) ('the Proposal')³ has **important data protection implications**.

5. Allocating the task of deciding to machines, on the basis of data, will create risks to the rights and freedoms of individuals, will impact their private lives and might harm groups or even societies as a whole. The EDPB and the EDPS emphasize that the rights to private life and to the protection of personal data, conflicting with the assumption of machines' decision autonomy underlying the concept of AI, are a pillar of EU values as recognized in the Universal Declaration of Human Rights (Article 12), the European Convention of Human Rights (Article 8) and the Charter of Fundamental Rights of the EU (hereinafter "the Charter") (Articles 7 and 8). Reconciling the perspective of growth offered by AI applications and the centrality and primacy of humans vis-a-vis machines is a very ambitious, yet necessary goal.
6. The EDPB and the EDPS welcome the involvement in the regulation of all stakeholders of the AI chain of value and the introduction of specific requirements for solution providers as they play a significant role in the products that make use of their systems. However, responsibilities of the various parties - user, provider, importer or distributor of an AI system - need to be clearly circumscribed and assigned. In particular, when processing personal data, special consideration should be given to the consistency of these roles and responsibilities with the notions of data controller and data processor carried by the data protection framework since both norms are not congruent.
7. The Proposal gives an important place to the notion of human oversight (Article 14) which the EDPB and the EDPS welcome. However, as stated earlier, due to the strong potential impact of certain AI systems for individuals or groups of individuals, real human centrality should leverage on highly qualified human oversight and a lawful processing as far as such systems are based on the processing of personal data or process personal data to fulfil their task so as to ensure that the right not to be subject to a decision based solely on automated processing is respected.
8. In addition, due to the data-intensive nature of many AI applications, the Proposal should promote the adoption of a data protection by design and by default approach at every level, encouraging the effective implementation of data protection principles (as envisaged in Article 25 GDPR and Article 27 EUDPR) by means of state-of-the-art technologies.
9. Lastly, the EDPB and the EDPS emphasize that this joint opinion is provided only as a preliminary analysis of the Proposal , without prejudice to any further assessment and opinion on the effects of the Proposal and it's compatibility with the EU data protection law.

³ COM(2021) 206 final.

2 ANALYSIS OF THE KEY PRINCIPLES OF THE PROPOSAL

2.1 Scope of the Proposal and relationship with the existing legal framework

10. According to the Explanatory Memorandum, the **legal basis** for the Proposal is in the first place Article 114 of the TFEU, which provides for the adoption of measures to ensure the establishment and functioning of the Internal Market⁴. In addition, the Proposal is based on Article 16 of the TFEU *insofar as it contains specific rules* on the protection of individuals with regard to the processing of personal data, notably restrictions of the use of AI systems for ‘real-time’ remote biometric identification in publicly accessible spaces for the purpose of law enforcement⁵.
11. The EDPB and EDPS recall that, in line with the jurisprudence of the CJEU, Article 16 TFEU provides an appropriate legal basis in cases where the protection of personal data is one of the essential aims or components of the rules adopted by the EU legislature⁶. The application of Article 16 TFEU also entails the need to ensure independent oversight for compliance with the requirements regarding the processing of personal data, as is also required Article 8 of the Charter.
12. The EDPS and EDPB recall that a comprehensive data protection framework adopted on the basis of Article 16 TFEU already exists, consisting of the General Data Protection Regulation (GDPR)⁷, the Data Protection Regulation for the European Union institutions, offices, bodies and agencies (EUDPR)⁸ and the Law Enforcement Directive (LED)⁹. According to the Proposal, it is only the additional restrictions regarding the processing of biometric data contained in the Proposal that may be considered as based on Article 16 TFEU and as therefore having the same legal basis as the GDPR, EUDPR or LED. This has important implications for the relationship of the Proposal to the GDPR, EUDPR and LED more generally, as set out below.
13. As regards the **scope of the Proposal**, the EDPB and EDPS strongly welcome the fact that the Proposal extends to the use of AI systems by EU institutions, bodies or agencies. Given that the use of AI systems by these entities may also have a significant impact on the fundamental

⁴ Explanatory memorandum, p. 5.

⁵ Explanatory memorandum, p. 6. See also recital (2) of the proposal.

⁶ Opinion of 26 July 2017, *PNR Canada*, Opinion procedure 1/15, ECLI:EU:C:2017:592, paragraph 96.

⁷ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016, p. 1–88.

⁸ Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39–98.

⁹ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131.

rights of individuals, similar to use within EU Member States, it is indispensable that the new regulatory framework for AI applies to both EU Member States and EU institutions, offices, bodies and agencies in order to ensure a coherent approach throughout the Union. As EU institutions, offices, bodies and agencies may act both as providers and users of AI systems, the EDPS and EDPB consider it fully appropriate to include these entities within the scope of the Proposal on the basis of Article 114 TFEU.

14. However, EDPB and EDPS have serious concerns regarding the exclusion of international law enforcement cooperation from the scope set out in Article 2(4) of the Proposal. This exclusion creates a significant risk of circumvention (e.g., third countries or international organisations operating high-risk applications relied on by public authorities in the EU).
15. The development and use of AI systems will in many cases involve the processing of personal data. Ensuring clarity of the relationship of this Proposal to the existing EU legislation on data protection is of utmost importance. The Proposal is without prejudice and complements the GDPR, the EUDPR and the LED. While the recitals of the Proposal clarify that the use of AI systems should still comply with data protection law, **the EDPB and EDPS strongly recommend clarifying in Article 1 of the Proposal that the Union's legislation for the protection of personal data**, in particular the GDPR, EUDPR, ePrivacy Directive¹⁰ and the LED, shall apply to any processing of personal data falling within the scope of the Proposal. A corresponding recital should equally clarify that the Proposal does not seek to affect the application of existing EU laws governing the processing of personal data, including the tasks and powers of the independent supervisory authorities competent to monitor compliance with those instruments.

2.2 Risk-based approach

16. The EDPB and the EDPS **welcome the risk-based approach** underpinning the Proposal. The Proposal would apply to any AI systems, including those which do not involve the processing of personal data but can still have an impact on interests or fundamental rights and freedoms.
17. The EDPB and the EDPS note that some of the provisions in the Proposal leave out the risks for groups of individuals or the society as a whole (e.g., collective effects with a particular relevance, like group discrimination or expression of political opinions in public spaces). The EDPB and the EDPS recommend that societal/group risks posed by AI systems should be equally assessed and mitigated.
18. The EDPB and the EDPS are of the view that the Proposal's risk-based approach should be clarified, and the concept of "risk to fundamental rights" **aligned with the GDPR**, insofar as aspects related to the protection of personal data come into play. Whether they are end-users, simply data subjects or other persons concerned by the AI system, the absence of any reference in the text to the individual affected by the AI system appears as a blind spot in the Proposal. Indeed, the obligations imposed on actors vis-a-vis the affected persons should emanate more

¹⁰ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) as amended by Directive 2006/24/EC and Directive 2009/136/EC.

concretely from the protection of the individual and her or his rights. Thus, the EDPB and the EDPS urge the legislators to explicitly address in the Proposal the **rights and remedies available to individuals** subject to AI systems.

19. The EDPB and EDPS take note of the choice of providing an exhaustive list of **high-risk AI systems**. This choice might create a black-and-white effect, with weak attraction capabilities of highly risky situations, undermining the overall risk-based approach underlying the Proposal. Also, this list of high-risk AI systems detailed in annexes II and III of the Proposal lacks some types of use cases which involve significant risks, such as the use of AI for determining the insurance premium, or for assessing medical treatments or for health research purposes. The EDPB and the EDPS also highlight that those annexes will need to be regularly updated to ensure that their scope is appropriate.
20. The Proposal requires the **providers** of the AI system to perform a risk assessment, however, in most cases, the (data) controllers will be the **users** rather than providers of the AI systems (e.g., a user of a facial recognition system is a ‘controller’ and therefore, is not bound by requirements on high-risk AI providers under the Proposal).
21. Moreover, it will **not always be possible for a provider to assess all uses** for the AI system. Thus, the initial risk assessment will be of a more general nature than the one performed by the user of the AI system. Even if the initial risk assessment by the provider does not indicate that the AI system is “high-risk” under the Proposal, this should not exclude a **subsequent (more granular) assessment** (data protection impact assessment (‘DPIA’) under Article 35 of the GDPR, Article 39 of EUDPR or under Article 27 of the LED) **that should be made by the user of the system**, considering the context of use and the specific use cases. The interpretation of whether under the GDPR, the EUDPR and the LED a type of processing is likely to result in a high-risk is to be made independently of the Proposal. However, the classification of an AI system as posing “high-risk” due to its impact on fundamental rights¹¹ **does trigger a presumption of “high-risk” under the GDPR, the EUDPR and the LED to the extent that personal data is processed**.
22. **The EDPB and the EDPS agree with the Proposal when it specifies that the classification of an AI system as high-risk does not necessarily mean that it is lawful *per se* and can be deployed by the user as such. Further requirements resulting from the EU data protection law may need to be complied with by the controller.** Furthermore, the underlying reasoning to Article 5 of the Proposal that, unlike prohibited systems, the high-risk systems may be permissible in principle is to be addressed and dispelled in the Proposal, especially since the proposed CE marking does not imply that the associated processing of personal data is lawful.
23. However, the compliance with legal obligations arising from Union legislation (including on the personal data protection) should be precondition to being allowed to enter the European

¹¹The European Union Agency for Fundamental Rights (FRA) has already addressed the need to conduct fundamental rights impact assessments when using AI or related technologies. In its 2020 report, “[Getting the future right – Artificial intelligence and fundamental rights](#)”, FRA identified “pitfalls in the use of AI, for example in predictive policing, medical diagnoses, social services, and targeted advertising” and stressed that “private and public organisations should carry out assessments of how AI could harm fundamental rights” to reduce negative impacts on individuals.

market as CE marked product. To this end, the EDPB and the EDPS **recommend including in Chapter 2 of Title III of the Proposal the requirement to ensure compliance with the GDPR and the EUDPR**. These requirements shall be audited (by third party audit) before the CE marking in line with the accountability principle. In the context of this third-party assessment, the initial impact assessment to be performed by the provider will be especially relevant.

24. Having regard to complexities triggered by the development of AI systems, it should be pointed out that the technical characteristics of AI systems (e.g., the type of AI approach) could result in greater risks. Therefore, any AI system risk assessment should consider **the technical characteristics along with its specific use cases and the context** in which the system operates.
25. In the light of the above, the EDPB and the EDPS recommend specifying in the Proposal that **the provider** shall perform an initial risk assessment on the AI system at stake **considering the use-cases** (to be specified in the Proposal - complementing for instance Annex III, 1(a), where the use-cases of AI biometric systems are not mentioned), and that the **user** of the AI system, in its quality of data controller under the EU data protection law (if relevant), shall perform the DPIA as detailed provided in Article 35 GDPR, Article 39 of the EUDPR and Article 27 LED, considering not only the technical characteristic and **the use case**, but **also the specific context** in which the AI will operate.
26. Moreover, some of the terms mentioned in Annex III of the Proposal, e.g. the term “essential private services” or small-scale provider using creditworthiness assessment AI for their own use, should be clarified.

2.3 Prohibited uses of AI

27. The EDPB and the EDPS consider that **intrusive forms of AI** – especially those who may affect human dignity – are to be seen as prohibited AI systems under Article 5 of the Proposal instead of simply being classified as “high-risk” in Annex III of the Proposal such as those under No. 6. This applies in particular to data comparisons that, on a large scale, also affect persons who have given no or only slight cause for police observation, or processing which impairs the principle of purpose limitation under data protection law. The use of AI in the area of police and law enforcement requires area-specific, precise, foreseeable and proportionate rules that need to consider the interests of the persons concerned and the effects on the functioning of a democratic society.
28. Article 5 of the Proposal risks paying lip service to the “values” and to the prohibition of AI systems in contrast with such values. Indeed, the criteria referred to under Article 5 to “qualify” the AI systems as prohibited **limit the scope of the prohibition** to such an extent that it could turn out to be meaningless in practice (e.g. “causes or is likely to cause [...] physical or psychological harm” in Article 5 (1) (a) and (b); limitation to public authorities in Article 5(1)(c); vague wording in and points (i) and (ii) under (c); limitation to “real time” remote biometric identification only without any clear definition etc.).
29. In particular, the use of AI for “social scoring”, as foreseen in Article 5(1) (c) of the Proposal, can lead to discrimination and is against the EU fundamental values. The Proposal only

prohibits these practices when conducted ‘over a certain period of time’ or ‘by public authorities or on their behalf’. Private companies, notably social media and cloud service providers, can process vast amounts of personal data and conduct social scoring. Consequently, **the Proposal should prohibit any type of social scoring**. It should be noted that in the law enforcement context, Article 4 LED already significantly limits – if not in practice prohibits – such type of activities.

30. **Remote biometric identification** of individuals in publicly accessible spaces poses a high-risk of intrusion into individuals’ private lives. Therefore, the EDPB and the EDPS **consider that a stricter approach is necessary**. The use of AI systems might present serious proportionality problems, since it might involve the processing of data of an indiscriminate and disproportionate number of data subjects for the identification of only a few individuals (e.g., passengers in airports and train stations). The **frictionless** nature of remote biometric identification systems also presents transparency problems and issues related to the legal basis for the processing under the EU law (the LED, the GDPR, the EUDPR and other applicable law). The problem regarding the way to properly inform individuals about this processing is still unsolved as well as the effective and timely exercise of the rights of individuals. The same applies to **its irreversible, severe effect on the populations’ (reasonable) expectation of being anonymous in public spaces**, resulting in a direct negative effect on the exercise of freedom of expression, of assembly, of association as well as freedom of movement.
31. Article 5(1)(d) of the Proposal provides an extensive **list of exceptional cases** in which ‘real-time’ remote biometric identification in publicly accessible spaces is permitted for the purpose of law enforcement. The EDPB and the EDPS consider **this approach flawed** on several aspects: First, it is unclear what should be understood as “a significant delay” and how should it be considered as a mitigating factor, taking into account that a mass identification system is able to identify thousands of individuals in only a few hours. In addition, the intrusiveness of the processing does not always depend on the identification being done in real-time or not. Post remote biometric identification in the context of a political protest is likely to have a significant chilling effect on the exercise of the fundamental rights and freedoms, such as freedom of assembly and association and more in general the founding principles of democracy. Second, the intrusiveness of the processing does not necessarily depend on its purpose. The use of this system for other purposes such as private security represents the same threats to the fundamental rights of respect for private and family life and protection of personal data. Lastly, even with the foreseen limitations, the potential number of suspects or perpetrators of crimes will almost always be “high enough” to justify the continuous use of AI systems for suspect detection, despite the further conditions in Article 5(2) to (4) of the Proposal. The reasoning behind the Proposal seems to omit that when monitoring open areas, the obligations under EU data protection law need to be met for not just suspects, but for all those that in practice are monitored.
32. For all these reasons, the EDPB and the EDPS **call for a general ban on any use of AI for an automated recognition of human features in publicly accessible spaces - such as of faces but also of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioral signals - in any context**. The current approach of the Proposal is to identify and list all AI

systems that should be prohibited. Thus, for consistency reasons, **AI systems for large-scale remote identification in online spaces** should be prohibited under Article 5 of the Proposal. Taking into account the LED, the EUDPR and GDPR, the EDPS and EDPB cannot discern how this type of practice would be able to meet the necessity and proportionality requirements, and that ultimately derives from what are considered acceptable interferences of fundamental rights by the CJEU and ECtHR.

33. Moreover, the EDPB and EDPS **recommend a ban**, for both public authorities and private entities, on **AI systems categorizing individuals from biometrics (for instance, from face recognition) into clusters according to ethnicity, gender, as well as political or sexual orientation, or other grounds for discrimination prohibited under Article 21 of the Charter, or AI systems whose scientific validity is not proven or which are in direct conflict with essential values of the EU (e.g., polygraph, Annex III, 6. (b) and 7. (a)).** Accordingly, “**biometric categorization**” should be **prohibited under Article 5.**
34. It also **affects human dignity to be determined or classified by a computer as to future behavior independent of one's own free will.** AI systems intended to be used by law enforcement authorities for making individual risk assessments of natural persons in order to assess the risk of a natural person for offending or reoffending criminal offences, cf. Annex III, 6. (a), or for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of a natural person or on assessing personality traits and characteristics or past criminal behavior, cf. Annex III, 6. (e) used according to their intended purpose will lead to pivotal subjection of police and judicial decision-making, thereby objectifying the human being affected. Such AI systems touching the essence of the right to human dignity should be prohibited under Article 5.
35. Furthermore, the EDPB and the EDPS consider that the use of AI to **infer emotions of a natural person is highly undesirable and should be prohibited**, except for certain well-specified use-cases, namely for health or research purposes (e.g., patients where emotion recognition is important), always with appropriate safeguards in place and of course, subject to all other data protection conditions and limits including purpose limitation.

2.4 High-risk AI systems

2.4.1 Need for an *ex-ante* conformity assessment by external third parties

36. The EDPB and the EDPS welcome that AI systems that pose a high-risk must be subject to a prior conformity assessment before they can be placed on the market or otherwise put into operation in the EU. In principle, this regulatory model is welcomed, as it offers a good balance between innovation-friendliness and a high level of proactive protection of fundamental rights. In order to be brought to use in specific environments like decision-making processes of public service institutions or critical infrastructure, ways to investigate the full source code must be laid out.
37. However, the EDPB and the EDPS advocate adapting the conformity assessment procedure under Article 43 of the Proposal to the effect that an ***ex ante* third-party conformity assessment must generally be carried out for high-risk AI.** Although a third-party

conformity assessment for high-risk processing of personal data is not a requirement in the GDPR or EUDPR, the risks posed by AI systems are yet to be fully understood. The general inclusion of an obligation for third-party conformity assessment would therefore further strengthen legal certainty and confidence in all high-risk AI systems.

2.4.2 Scope of regulation must also cover AI systems already in use

38. According to Article 43(4) of the Proposal, high-risk AI systems should be subject to a new conformity assessment procedure whenever a significant change is made. It is right to ensure that AI systems comply with the requirements of the AI Regulation throughout their lifecycle. AI systems that have been placed on the market or put into service before application of the proposed regulation (or 12 months thereafter for large-scale IT systems listed in Annex IX) are excluded from their scope, unless those systems are subject to ‘significant changes’ in design or intended purpose (Article 83).
39. Yet, the threshold for ‘significant changes’ is unclear. Recital 66 of the Proposal specifies a lower threshold for conformity re-assessment “whenever a change occurs which may affect the compliance”. A similar threshold would be appropriate for Article 83, at least for high-risk AI systems. Additionally, in order to close any protection gaps, it is necessary that AI systems already established and in operation - after a certain implementation phase - also comply with all requirements of the AI Regulation.
40. The manifold possibilities of personal data processing and external risks affect the security of AI systems, too. The focus of Article 83 on “significant changes in design or intended purpose” does not include a reference to changes in external risks. A reference to changes of the threats-scenario, arising from external risks, e.g., cyber-attacks, adversarial attacks and substantiated complaints from consumers therefore should be included in Article 83 of the Proposal.
41. Moreover, as the entry into application is envisaged for 24 months following the entry into force of the future Regulation, the EDPS and EDPB do not consider it appropriate to exempt AI systems already placed on the market for an even longer period of time. While the Proposal also provides that the requirements of the Regulation shall be taken into account in the evaluation of each large-scale IT system as provided by the legal acts listed in Annex IX, the EDPB and EDPS consider that requirements concerning the putting into service use of AI systems should be applicable from the date of application of the future Regulation.

2.5 Governance and European AI Board

2.5.1 Governance

42. The EDPB and the EDPS welcome the designation of the EDPS as the competent authority and the market surveillance authority for the supervision of the Union institutions, agencies and bodies when they fall within the scope of this Proposal. The EDPS stands ready to fulfil its new role as the AI regulator for the EU public administration. Moreover, the role and tasks of the EDPS are not sufficiently detailed and should be further clarified in the Proposal, specifically when it comes to its role as market surveillance authority.

43. The EDPB and the EDPS acknowledge the allocation of financial resources, which is foreseen for the Board and the EDPS, acting as a notifying body, in the Proposal. However, the fulfillment of the new duties foreseen for the EDPS, whether when acting as notified body, would require significantly higher financial and human resources.
44. Firstly, because the wording of Article 63 (6) states that the EDPS “shall act as market surveillance authority” for Union institutions, agencies and bodies that fall within the scope of the Proposal, which does not clarify if EDPS is to be considered a fully embodied “market surveillance authority”, as foreseen in Regulation (EU) 2019/1020. This raises questions about the duties and powers of the EDPS in practice. Secondly, and provided that the former question is answered affirmatively, it is unclear how the role of the EDPS, as foreseen in EUDPR can accommodate the task foreseen in Article 11 of the Regulation (EU) 2019/1020, which include “effective market surveillance within their territory of products made available online” or “physical and laboratory checks based on adequate samples”. There is the risk that taking up the new set of tasks without further clarifications in the Proposal might endanger the fulfillment of its obligations as data protection supervisor.
45. However, the EDPB and the EDPS underline that some provisions of the Proposal defining the tasks and powers of the different competent authorities under the AI regulation, their relationships, their nature and the guarantee of their independence seem unclear at this stage. Whereas Regulation 2019/1020 states that market surveillance authority must be independent, the draft regulation does not require Supervisory authorities to be independent, and even requires them to report to the Commission on certain tasks carried out by market surveillance authorities, which can be different institutions. Since the proposal also states that DPAs will be the market surveillance authorities for AI systems used for law enforcement purposes (Article 63 (5)) it also means that they will be, possibly via their national supervisory authority, subject to reporting obligations to the Commission (Article 63 (2)), which seems incompatible with their independency.
46. Therefore, the EDPB and the EDPS consider that those provisions need to be clarified in order to be consistent with Regulation 2019/1020, EUDPR and the GDPR, and the Proposal should clearly establish that Supervisory authorities under the AI Regulation must be completely independent in the performance of their tasks, since this would be an essential guarantee for the proper supervision and enforcement of the future Regulation.
47. The EDPB and the EDPS would also like to recall that data protection authorities (DPAs) are already enforcing the GDPR, the EUDPR and the LED on AI systems involving personal data in order to ensure the protection of fundamental rights and more specifically the right to data protection. Therefore, DPAs already have to some extent, as required in the Proposal for the national supervisory authorities, an understanding of AI technologies, data and data computing, fundamental rights, as well as an expertise in assessing risks to fundamental rights posed by new technologies. In addition, when AI systems are based on the processing of personal data or process personal data, provisions of the Proposal are directly intertwined with the data protection legal framework, which will be the case for most of the AI systems in the scope of the regulation. As a result, there will be interconnections of competencies between supervisory authorities under the Proposal and DPAs.

48. Hence, the designation of DPAs as the national supervisory authorities would ensure a more harmonized regulatory approach, and contribute to the consistent interpretation of data processing provisions and avoid contradictions in its enforcement among Member States. It would also benefit all stakeholders of the AI chain of value to have a single contact point for all personal data processing operations falling within the scope the Proposal and limit the interactions between two different regulatory bodies for processing that are concerned by the Proposal and GDPR. As a consequence, the EDPB and the EDPS consider that **DPAs should be designated as the national supervisory authorities pursuant to Article 59 of the Proposal.**
49. In any event, insofar as the Proposal contains specific rules on the protection of individuals with regard to the processing of personal data adopted on the basis of Article 16 TFEU, compliance with these rules, notably restrictions of the use of AI systems for ‘real-time’ remote biometric identification in publicly accessible spaces for the purpose of law enforcement, **must be subject to the control of independent authorities.**
50. However, there is no explicit provision in the Proposal that would assign competence for ensuring compliance with these rules to the control of independent authorities. The only reference to competent data protection supervisory authorities under GDPR, or LED is in Article 63(5) of the Proposal, but only as “market surveillance” bodies and alternatively with some other authorities. The EDPB and the EDPS consider that this set up does not ensure compliance with the requirement of independent control set out in Article 16(2) TFEU and Article 8 of the Charter.

2.5.2 The European AI Board

51. The Proposal establishes a “European Artificial Intelligence Board” (EAIB). The EDPB and the EDPS recognize the need for a consistent and harmonized application of the proposed framework, as well as the involvement of independent experts in the development of the EU policy on AI. At the same time, the Proposal foresees to give a predominant role to the Commission. Indeed, not only would the latter be part of the EAIB but it would also chair it and have a right of veto for the adoption of the EAIB rules of procedure. This contrasts with the need for an AI European body independent from any political influence. Therefore, the EDPB and the EDPS consider that the future AI Regulation should give **more autonomy to the EAIB**, in order to allow it to truly ensure the consistent application of the regulation across the single market
52. The EDPB and the EDPS also note that no power is conferred to the EAIB regarding the enforcement of the proposed Regulation. Yet, considering the spread of AI systems across the single market and the likelihood of cross-border cases, there is a crucial need for a harmonized enforcement and a proper allocation of competence between national supervisory authorities. The EDPB and the EDPS therefore recommend that the cooperation mechanisms between national supervisory authorities be specified in the future AI Regulation. The EDPB and EDPS suggest to impose a mechanism guaranteeing a single point of contact for individuals concerned by the legislation as well as for companies, for each AI system, and that for organisations whose

activity covers more than half of the Member States of the EU, the EAIB may designate the national authority that will be responsible for enforcing the AI Regulation for this AI system.

53. Furthermore, considering the independent nature of the authorities that shall compose the Board, the latter shall be entitled to act on its own initiative and not only to provide advice and assistance to the Commission. The EDPB and the EDPS therefore stress the need for an extension of the mission assigned to the Board, which in addition does not correspond to the tasks listed by the Proposal.
54. To satisfy those purposes, the **EAIB shall have sufficient and appropriate powers**, and its legal status should be clarified. In particular, for the material scope of the future Regulation to remain relevant, it seems necessary to involve the authorities in charge of its application in its evolution. Hence, the EDPB and the EDPS recommend that the EAIB should be empowered to propose to the Commission amendments of the annex I defining the AI techniques and approaches and of the annex III listing the high-risk AI systems referred to in article 6(2). The EAIB should also be consulted by the Commission prior any amendment of those annexes.
55. Article 57(4) of the Proposal foresees exchanges between the Board and other Union bodies, offices, agencies and advisory groups. Taking into account their previous work in the field of AI and their human rights expertise, the EDPB and EDPS recommend to consider the Fundamental Rights Agency as one of the observers to the Board.

3 INTERACTION WITH THE DATA PROTECTION FRAMEWORK

3.1 Relationship of the Proposal to the existing EU data protection law

56. A clearly defined relationship between the Proposal and existing data protection law is an essential prerequisite to ensure and uphold the respect and application of the EU acquis in the field of personal data protection. Such EU law, in particular the GDPR, the EUDPR and the LED, has to be considered as a prerequisite on which further legislative proposals may build upon without affecting or interfering with the existing provisions, including when it comes to the competence of supervisory authorities and governance.
57. In the view of the EDPB and the EDPS, it is therefore important to clearly avoid in the Proposal any inconsistency and possible conflict with the GDPR, the EUDPR and the LED. This not only for the sake of legal certainty, but also to avoid that the Proposal has the effect of directly or indirectly jeopardizing the fundamental right to the protection of personal data, as established under Article 16 of the TFEU and Article 8 of the Charter.
58. In particular, self-learning machines could protect the personal data of individuals only if this is embedded by conception. The immediate possibility of exercising the rights of individuals under Article 22 (Automated individual decision-making, including profiling) GDPR or Article 23 EUDPR, regardless of the purposes of processing, is also essential. In this regard, other rights of the data subjects related to the right of deletion, the right of correction according to

the data protection legislation, must be provided in the AI systems from the very beginning, whatever the chosen AI approach or the technical architecture.

59. Using personal data for AI systems learning may lead to the generation of biased decision-making patterns at the core of the AI system. Thus, various safeguards and in particular a qualified human oversight in such processes should be required to ensure that data subjects rights are respected and guaranteed, as well as to avoid any and all negative effects for individuals. Competent authorities should also be able to propose guidelines to assess bias in AI systems and assist the exercise of human oversight.
60. Data subjects should always be informed when their data is used for AI training and / or prediction, of the legal basis for such processing, general explanation of the logic (procedure) and scope of the AI-system. In that regard, individuals' right of restriction of processing (Article 18 GDPR and Article 20 EUDPR) as well as deletion / erasure of data (Article 16 GDPR and Article 19 EUDPR) should always be guaranteed in those cases. Furthermore, the controller should have explicit obligation to inform data subject of the applicable periods for objection, restriction, deletion of data etc. The AI system must be able to meet all data protection requirements through adequate technical and organizational measures. A right to explanation should provide for additional transparency.

3.2 Sandbox & further processing (Articles 53 and 54 of the Proposal)

61. Within the existing legal and moral boundaries, it is important to promote European innovation through tools such as a sandbox. A sandbox gives the opportunity to provide safeguards needed to build trust and reliance on AI systems. In complex environments, it may be difficult for AI practitioners to weigh all interests in a proper manner. Especially for small and medium enterprises with limited resources, operating in a regulatory sandbox may yield quicker insights and hence foster innovation.
62. Article 53, section 3 of the Proposal states that the sandbox does not affect supervisory and corrective powers. If this clarification is useful, there is also a need for the production of direction or guidance on how to strike a good balance between being a supervisory authority on the one hand and giving detailed guidance through a sandbox on the other.
63. Article 53, section 6 describes that the modalities and conditions of the operation of the sandboxes shall be set out in implementing acts. It is important that specific guidelines be produced in order to ensure consistency and support in the establishment and operation of sandboxes. However, binding implementing acts could limit each Member State's ability to customise the sandbox according to their needs and local practices. Thus, the EDPB and the EDPS recommend that the EAIB should provide guidelines for sandboxes instead.
64. Article 54 of the Proposal seeks to provide a legal basis for further processing of personal data for developing certain AI systems in the public interest in the AI regulatory sandbox. The relationship of Article 54(1) of the Proposal to Article 54(2) and recital 41 of the Proposal and thus also to existing EU data protection law remains unclear. However, the GDPR and the EUDPR already have an established basis for 'further processing'. Especially with regard to

cases where it is in the public interest to allow further processing; balancing between the controller's interests and the data subject's interests do not have to hinder innovation. The Article 54 of the Proposal currently does not address two important issues (i) under what circumstances, using which (additional) criteria are the interests of data subjects weighed, and (ii) whether these AI systems will only be used within the sandbox. The EDPB and the EDPS welcomes the requirement for a Union or Member State law when processing personal data collected under the LED in a sandbox, but recommend to further specify what is envisaged here, in a manner that aligns with the GDPR and the EUDPR, mainly by clarifying that the legal basis of such sandboxes should comply with the requirements established in Articles 23 (2) GDPR, 25 EUDPR, and precise that every use of the sandbox must undergo a thorough evaluation. This also applies to the full list of conditions from Article 54(1) point (b to j).

65. Some additional considerations regarding the reuse of data in Article 54 of the Proposal indicate that operating a sandbox is resource intensive and that it is therefore realistic to estimate that only a small number of businesses would get the chance to participate. Participating in the sandbox could be a competitive advantage. Enabling reuse of data would require careful consideration of how to select participants to ensure they are within the scope and to avoid unfair treatment. The EDPB and the EDPS are concerned that enabling reuse of data within the framework of the sandbox diverges from the accountability approach in the GDPR, where the accountability is placed on the data controller, not on the competent authority.
66. Furthermore, the EDPB and the EDPS consider that given the objectives of the sandbox, which are to develop, test and validate AI systems, the sandboxes cannot fall within the scope of the LED. While the LED provides for the reuse of data for scientific research, the data processed for that secondary purpose will be subject to GDPR or EUDPR and no longer to LED.
67. It is not clear what a regulatory sandbox will encompass. The question arises whether the proposed regulatory sandbox includes an IT infrastructure in each Member State with some additional legal grounds for further processing, or whether it merely organizes access to regulatory expertise and guidance. The EDPB and the EDPS urge the legislator to clarify this concept in the Proposal and to clearly state in the Proposal that the regulatory sandbox does not imply an obligation on competent authorities to provide its technical infrastructure. In any cases, financial and human resources must be provided to the competent authorities accordingly to such clarification.
68. Finally, the EDPB and the EDPS would like to emphasize the development of cross-border AI-systems that will be available to the European Digital Single Market as a whole. In the case of such AI-systems, the regulatory sandbox as a tool for innovation should not become a hindrance for cross-border development. Therefore, the EDPB and the EDPS recommend a coordinated cross-border approach that is still sufficiently available at a national level for all SME's, offering a common framework across Europe without being too restrictive. A balance between European coordination and national procedures must be struck in order to avoid conflicting implementation of the future AI Regulation which would hinder EU-wide innovation.

3.3 Transparency

69. The EDPB and the EDPS welcome that high-risk AI systems shall be registered in a public database (referred to under Article 51 and 60 of the Proposal). This database should be taken as an opportunity to provide information for the public at large on the scope of application of AI system and on known flaws and incidents that might compromise their functioning and the remedies adopted by providers to address and fix them.
70. A key democratic principle is the use of checks and balances. Therefore, the fact that the transparency obligation does not apply to AI systems used to detect, prevent, investigate, or prosecute criminal offences is too broad of an exception. A distinction must be made between AI systems that are used to detect or prevent and AI systems that aim to investigate or help the prosecution of criminal offenses. Safeguards for prevention and detection have to be stronger because of the presumption of innocence. Moreover, the EDPB and the EDPS regret the absence of cautionary warnings in the proposal, which can be interpreted as a greenlight for the use of even unproven, high-risk AI systems or applications.
71. In those cases where little to no transparency can be given to the public due to reasons of secrecy, even in a well-functioning democracy, safeguards should be in place and those AI systems should be registered with and provide transparency to the competent supervisory authority.
72. Ensuring transparency in AI systems is a very challenging goal. The fully quantitative decision-making approach of many AI systems, inherently different from human approach mostly relying on causal and theoretical reasoning, may conflict with the need to get a prior understandable explanation of machine outcomes. The Regulation should promote new, more proactive and timely ways to inform users of AI systems on the (decision-making) status where the system lays at any time, providing early warning of potential harmful outcomes, so that individuals whose right and freedoms may be impaired by machine's autonomous decisions may react, or redress the decision.

3.4 Processing of special categories of data & data relating to criminal offences

73. The processing of special categories of data in the area of law enforcement is governed by the provisions of the EU data protection framework, including the LED as well as its national implementation. The Proposal claims not to provide a general legal ground for processing of personal data, including special categories of personal data, cf. recital 41. At the same time, Article 10 (5) of the Proposal reads “the providers of such systems may process special categories of personal data”. Furthermore, the same provision requires additional safeguards, also giving examples. Thereby, the Proposal seems to interfere with the application of the GDPR, the LED and the EUDPR. While the EDPB and the EDPS welcome the attempt to arrange for adequate safeguards, a more coherent regulatory approach is needed, as the current provisions do not seem sufficiently clear to create a legal basis for the processing of special categories of data, and need to be complemented with additional protective measures that still need to be assessed. Moreover, when personal data have been collected by processing within the scope of the LED the possible additional safeguards and limitations stemming from the national transpositions of the LED will need to be taken into account.

3.5 Compliance mechanisms

3.5.1 Certification

74. One of the main pillars of the Proposal is certification. The certification system outlined in the Proposal is based on a structure of entities (Notifying Authorities/Notified Bodies/Commission) and a conformity assessment/certification mechanism covering the mandatory requirements applicable to high-risk AI systems, and based on European harmonized standards under Regulation (EU) No 1025/2012 and common specifications to be established by the Commission. This mechanism is different from the certification system aimed at ensuring compliance with data protection rules and principles, outlined in Articles 42 and 43 of the GDPR. It is however not clear how certificates issued by notified bodies in accordance with the Proposal may interface with data protection certifications, seals and marks provided for by the GDPR, unlike what it is provided for other types of certifications (see Article 42(2) with regard to certifications issued under Regulation (EU) 2019/881).
75. As far as high-risk AI systems are based on the processing of personal data or process personal data to fulfil their task, these misalignments may generate legal uncertainties for all concerned bodies, since they may lead to situations in which AI systems, certified under the Proposal and marked with a CE marking of conformity, once placed on the market or put into service, might be used in a way which is not compliant with the rules and principles of data protection.
76. The Proposal is missing a clear relation to the data protection law as well as other EU and Member States law applicable to each ‘area’ of high-risk AI system listed in Annex III. In particular, the proposal should include the principles of data minimization and data protection by design as one of the aspects to take into consideration before obtaining the CE marking, given the possible high level of interference of the high-risk AI systems with the fundamental rights to privacy and to the protection of personal data, and the need to ensure a high level of trust in the AI system. Therefore, the EDPB and the EDPS recommend amending the Proposal so as to clarify the relationship between certificates issued under the said Regulation and data protection certifications, seals and marks. Lastly, the data protection authorities should be involved in the preparation and establishment of harmonized standards and common specifications.
77. In connection with Article 43 of the Proposal, relating to the conformity assessment, the derogation from the conformity assessment procedure set out in Article 47 seems to be very broad including too many exceptions such as reasons of exceptional reasons of public security or the protection of life and health of persons, environmental protection and the protection of key industrial and infrastructural assets. We would propose the legislators to narrow them down.

3.5.2 Codes of conduct

78. According to Article 69 of the Proposal, the Commission and the Member States shall encourage and facilitate the drawing up of codes of conduct (CoCs) intended to foster the voluntary application by providers of non-high-risk AI systems of the requirements applicable to high-risk AI systems, as well as additional requirements. In line with recital 78 of the GDPR, the EDPB and the EDPS recommend identifying and defining synergies between these instruments and the

codes of conduct provided for by the GDPR which support data protection compliance. In this context, it is relevant to clarify if the protection of personal data is to be considered among “additional requirements” that can be addressed by the CoCs referred to in paragraph 2 of Article 69. It is also relevant to ensure that the “technical specifications and solutions”, addressed by the CoCs referred to in paragraph 1 of Article 69, as designed to foster compliance with the requirements of the AI draft Regulation, do not conflict with the rules and principles of the GDPR and the EUDPR. By doing so, adherence to these tools by providers of non-high-risk AI systems - as far as such systems are based on the processing of personal data or process personal data to fulfil their task - would represent an added value, since this will ensure that controller and processors will be able to fulfil their data protection obligations in the use of those systems.

79. At the same time, the legal framework for trustworthy AI would result complemented by the integration of CoCs, so as to foster trust in the use of this technology in a way that is safe and compliant with the law, including the respect of fundamental rights. However, the design of these instruments should be strengthened by envisaging mechanisms aimed at verifying that such codes provide effective “technical specifications and solutions” and set out “clear objectives and key performance indicators to measure the achievement of those objectives” as integral parts of the codes in question. Moreover, the absence of any reference to (mandatory) monitoring mechanisms for codes of conduct designed to verify that providers of non-high-risk AI systems comply with their provisions, as well as the possibility for individual providers to draw up (and implement themselves) the said codes (see section 5.2.7 of the explanatory memorandum) may further weaken the efficacy and enforceability of these instruments.
80. Lastly, the EDPB and the EDPS ask for clarifications with regard to the types of initiatives the Commission may develop, according to recital 81 of the Proposal, “to facilitate the lowering of technical barriers hindering cross-border exchange of data for AI development”.

4 CONCLUSION

81. Even though the EDPB and the EDPS welcome the Proposal of the Commission and consider that such a regulation is necessary to guarantee the fundamental rights of EU citizens and residents, they consider that the Proposal needs to be adapted on several issues, to ensure its applicability and efficiency.
82. Given the complexity of the Proposal as well as the issues it aims to tackle, a lot of work remains to be done until the Proposal can give birth to a well-functioning legal framework, efficiently supplementing the GDPR in protecting basic human rights while fostering innovation. The EDPB and the EDPS will continue to be available to offer their support in this journey.

Brussels, 18 June 2021

For the European Data Protection Board

The Chair

Andrea JELINEK

For the European Data Protection Supervisor

The Supervisor

Wojciech Rafał WIEWIÓROWSKI



**EDPB-EDPS Joint Opinion
03/2021 on the Proposal for a
regulation of the European
Parliament and of the
Council on European data
governance (Data
Governance Act)**

Version 1.1

Version history

Version 1.1	09 June 2021	Minor editorial changes
Version 1.0	10 March 2021	Adoption of the Joint Opinion

Adopted

TABLE OF CONTENTS

1	BACKGROUND	5
2	SCOPE OF THE JOINT OPINION.....	6
3	ASSESSMENT	8
3.1	General remarks.....	8
3.2	General issues related to the relationship of the Proposal with Union law in the field of personal data protection	9
3.3	Re-use of certain categories of protected data held by public sector bodies	18
3.3.1	Relationship of the Proposal with the Open Data Directive and with the GDPR	18
3.3.2	Article 5: conditions for re-use of data by public sector bodies	20
3.3.3	Article 5(11): re-use of “highly sensitive” non-personal data.....	25
3.3.4	Article 6: fees for data re-use	25
3.3.5	Governance and institutional aspects: Article 7 (competent bodies). Article 8 (single information point).....	26
3.4	Requirements applicable to data sharing service providers.....	28
3.4.1	Data intermediaries under Article 9(1) (b): intermediation services between data subjects and potential data users.	31
3.4.2	Data intermediaries under Article 9(1) (c): ‘data cooperatives’	33
3.4.3	Article 10: notification regime - general requirements to be eligible for registration - content of the notification; outcome (and timing) of the notification. Article 11: conditions for providing data sharing services.....	34
3.4.4	Articles 12 and 13: competent authorities and monitoring of compliance (with Articles 10 and 11).....	37
3.5	Data altruism.....	39
3.5.1	Interplay between data altruism and consent under the GDPR.....	39
3.5.2	Articles 16-17: registration regime - general requirements to be eligible for registration - content of the registration; outcome (and timing) of the registration;	42
3.5.3	Articles 18-19: transparency requirements and “specific requirements to safeguard rights and interests of data subjects and legal entities as regards their data”.....	43
3.5.4	Articles 20 and 21: competent authorities for registration and monitoring of compliance	45
3.5.5	Article 22: European data altruism consent form.....	46
3.6	International transfers of data: Article 5(9)-(13); recital 17, 19; Article 30.....	46

3.7	Horizontal provisions on institutional settings; complaints; European Data Innovation Board (EDIB) expert group; delegated acts; penalties, evaluation and review, amendments to the single digital gateway regulation, transitional measures and entry into force	48
3.7.1	Article 23: requirements relating to competent authorities	48
3.7.2	Article 24: complaints; Article 25: right to effective judicial remedy	49
3.7.3	Articles 26 and 27: composition and tasks of the European Data Innovation Board Expert Group	49
3.7.4	Article 31: penalties for infringements of the Proposal, to be applied	51
3.7.5	Article 33: amendment to Regulation (EU) 2018/1724	51

The European Data Protection Board and the European Data Protection Supervisor

Having regard to Article 42(2) of the Regulation 2018/1725 of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC ("EUDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

HAVE ADOPTED THE FOLLOWING JOINT OPINION

1 BACKGROUND

1. The Proposal for Data Governance Act ("the Proposal") is enacted pursuant to the Communication "A European strategy for data" ("the Data Strategy").¹
2. The European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) notice that, according to the Commission, the Data Strategy provides that "*citizens will trust and embrace data-driven innovation only if they are confident that any personal data sharing in the EU will be subject to full compliance with the EU's strict data protection rules*".²
3. As specified in its Explanatory Memorandum, the Proposal "*aims to foster the availability of data for use by increasing trust in data intermediaries and by strengthening data-sharing mechanisms across the EU. The instrument would address the following situations:*"
 - *Making public sector data available for re-use, in situations where such data is subject to rights of others.*
 - *Sharing of data among businesses, against remuneration in any form.*
 - *Allowing personal data to be used with the help of a 'personal data-sharing intermediary', designed to help individuals exercise their rights under the General Data Protection Regulation (GDPR).*
 - *Allowing data use on altruistic grounds*"³.
4. When presenting the Proposal, the Commission has notably considered that "*the new regulation will provide a good governance framework supporting the common European data spaces and will ensure that data can be made available voluntarily by data holders. It will complement the upcoming rules on*

¹ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions "A European strategy for data", 19 of February 2020, COM (2020) 66 final.

² A European strategy for data, Introduction, page 1.

³ Explanatory Memorandum, page 1.

high-value datasets under the Open Data Directive which will ensure access to certain datasets across the EU for free, in machine-readable format and through standardised Application Programming Interfaces (APIs)"⁴.

5. The Data Strategy also highlights that "*The availability of data is essential for training artificial intelligence systems, with products and services rapidly moving from pattern recognition and insight generation to more sophisticated forecasting techniques and, thus, better decisions"*⁵.
6. As acknowledged in the Explanatory Memorandum of the Proposal, "*the interplay with the legislation on personal data is particularly important. With the General Data Protection Regulation (GDPR) and ePrivacy Directive, the EU has put in place a solid and trusted legal framework for the protection of personal data and a standard for the world"*⁶.
7. The EDPB and the EDPS also point out that the Proposal, as referred to in the Explanatory Memorandum, "*aims at facilitating data sharing including by reinforcing trust in data sharing intermediaries that are expected to be used in the different data spaces. It does not aim to grant, amend or remove the substantial rights on access and use of data. This type of measures is envisaged for a potential Data Act (2021)"*⁷. At the time of drafting this Joint Opinion, the aim and content of such Data Act are not yet available.

2 SCOPE OF THE JOINT OPINION

8. On 25 November 2020, the Commission published the Proposal for a regulation of the European Parliament and of the Council on European data governance ("Data Governance Act") ("the Proposal").
9. On 25 November 2020, the Commission requested a Joint Opinion of the EDPB and the EDPS on the basis of Article 42(2) of Regulation (EU) 2018/1725 (EUDPR) on the Proposal.
10. **The Proposal is of particular importance for the protection of individuals' rights and freedoms with regard to the processing of personal data. The scope of this opinion is limited to the aspects of the Proposal related to the protection of personal data, which, as observed, represent a key -if not the most important- aspect of the Proposal.**
11. In this regard, the EDPB and the EDPS notice that recital (3) provides that "*This Regulation is therefore without prejudice to Regulation (EU) 2016/679*".
12. The EDPB and the EDPS consider that the underlying objective of reinforcing trust with a view to facilitate data availability and benefit the digital economy in the EU is indeed grounded in **the need to ensure and uphold the respect and application of the EU acquis in the field of personal data**

⁴ https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2103#European%20Data%20Spaces

⁵ Data Strategy, pages 2 and 3.

⁶ Explanatory Memorandum, page 1.

⁷ Explanatory Memorandum, page 1.

protection. Applicable EU law in such field, and in particular Regulation EU 2016/679 (General Data Protection Regulation, GDPR), shall be considered as a prerequisite on which further legislative proposals may build upon without affecting or interfering with the relevant existing provisions, including when it comes to the competence of supervisory authorities and other governance aspects.⁸.

13. In the view of the EDPB and the EDPS, it is therefore important to **clearly avoid in the legal text of the Proposal any inconsistency and possible conflict with the GDPR**. This not only for the sake of legal certainty, but also to avoid that the Proposal has the effect of directly or indirectly jeopardizing the fundamental right to the protection of personal data, as established under Article 16 of the Treaty on the Functioning of the European Union (TFEU) and Article 8 of the Charter of fundamental rights of the European Union.
14. In particular, in this Joint Opinion, the EDPB and the EDPS point out to inconsistencies with the EU data protection legislation (as well as with other EU legislation, such as the Open Data Directive) and to problems, relating for instance to legal certainty, that would arise from the entry into force of the current Proposal.
15. Since the Proposal, as detailed in this Joint Opinion, raises a significant number of serious concerns, often intertwined, related to the protection of the fundamental right to the protection of personal data, **it is not the aim of this Joint Opinion to provide an exhaustive list of issues to be addressed by the legislators, nor always alternative proposals or wording suggestions**. Instead, **this Joint Opinion aims at addressing the main criticalities of the Proposal**. At the same time, the EDPB and the EDPS remain available to provide further clarifications and exchanges with the Commission.
16. The EDPB and the EDPS are also aware that the legislative process on the Proposal is ongoing and stress their **availability to the co-legislators to provide further advice and recommendations throughout this process**, to ensure in particular: legal certainty for natural persons, economic operators and public authorities; due protection of personal data for data subjects in line with the TFEU, the Charter of Fundamental Rights of the EU and the data protection acquis; a sustainable digital environment including the necessary ‘checks and balances’.
17. This call for the involvement of data protection authorities also relates, due to the possible important links with the Proposal⁹, to any forthcoming proposal for a European Data Act.

⁸ See EDPS Opinion 3/2020 on the European strategy for data, at paragraph 64: “Finally, the EDPS underlines that in the context of future governance mechanisms the competences of the **independent supervisory authorities for data protection** must be properly respected. Moreover, the implementation of the Strategy leading to wider use of data will require a **significant increase of resources for DPAs** and other public oversight bodies, in particular in terms of **technical expertise and capabilities**. Cooperation and joint investigations between all relevant public oversight bodies, including data protection supervisory authorities, should be encouraged.”

⁹ The Impact Assessment accompanying the Proposal, SWD (2020) 295 final, specifies at page 6 that (bold added): “The current initiative is a **first step in the two-step approach** announced in the European Strategy for Data. **The initiative will address the urgent need to facilitate data sharing through an enabling governance framework. In a second step**, the Commission will address issues about **who controls or ‘owns’ the data**, i.e. **the material rights on who can access and use what data under which circumstances**. The **introduction of such rights** will be examined in the context of the **Data Act (2021)**. Diverging interests of the stakeholders and

3 ASSESSMENT

3.1 General remarks

18. The EDPB and the EDPS acknowledge the legitimate objective of fostering the availability of data for use by increasing trust in data intermediaries and by strengthening data-sharing mechanisms across the EU, while highlighting that the protection of personal data is an essential and integral element of the trust individuals and organizations should have in the development of the digital economy. The proposal for a regulation on European Data Governance (Data Governance Act) is also to be considered in the light of the increased reliance of the digital economy on the processing of personal data and of the development of new technologies such as large data set analytics and artificial intelligence.
19. The EDPB and the EDPS underline that, whereas the GDPR was built upon the need to reinforce the fundamental right to data protection, the Proposal clearly focuses on unleashing the economic potential of data re-use and sharing. Thus, the Proposal intends to “improve the conditions for data sharing in the internal market”, as stated in Recital (3). However, **the EDPB and the EDPS note that the Proposal, also having regard to the Impact Assessment accompanying it, does not duly take into account the need to ensure and guarantee the level of protection of personal data provided under EU law. The EDPB and the EDPS consider that this policy trend toward a data-driven economy framework without a sufficient consideration of personal data protection aspects raises serious concerns from a fundamental rights viewpoint.** In this regard, the EDPB and the EDPS emphasise that any proposal, including upcoming initiatives related to data, such as the European Data Act, that may have an impact on the processing of personal data, must ensure and uphold the respect and application of the EU acquis in the field of personal data protection.
20. **The EDPB and the EDPS furthermore highlight that the European Union model relies on the mainstreaming of its values and fundamental rights within its policy developments, and that the GDPR must be considered as a foundation on which to build a European data governance model. As already stated in various policy contexts, such as the fight against the COVID-19 pandemic, the EU legal framework in the field of personal data protection shall be considered as an enabler, rather than an obstacle, to the development of a data economy that corresponds to the Union values and principles.**
21. The EDPB and the EDPS trusts this Joint Opinion will inform the co-legislators in ensuring the adoption of a legislative instrument which is fully compliant with the EU acquis in the field of personal data protection and therefore increases trust by upholding the level of protection provided by EU law under the supervision of the independent Data Protection Authorities established under Article 16(2) TFEU.

different views on what is fair in this respect make these issues subject to intense debate, which warrants taking more time.”

3.2 General issues related to the relationship of the Proposal with Union law in the field of personal data protection

22. The Proposal contains several references to compliance with the GDPR – which lays down the rules relating to the protection of natural persons with regard to the processing of personal data and to the free movement of personal data (see, among others, recital (3); recital (28) of the Proposal: “*when the data sharing service providers are data controllers or processors in the sense of Regulation (EU) 2016/679 they are bound by the rules of that Regulation.*”).
23. The EDPB and the EDPS consider that, in light of the scope of the processing of personal data to which the Proposal makes reference, recital 3 should also include a reference to Directive (EC) 2002/58 (“ePrivacy Directive”), as it is also part of the EU acquis in the field of personal data protection with which the Proposal shall be in compliance, consistent.
24. More in general, the EDPB and the EDPS consider that **both the spirit and the letter of the Proposal must not undermine the level of protection and ensure full consistency with all the principles and rules** established by the GDPR to effectively guarantee the fundamental rights to the protection of personal data provided under Article 8 of the Charter and Article 16 TFEU.
25. Having regard to the above, as referred to in the following paragraphs of this Joint Opinion, the EDPB and the EDPS consider that **the Proposal raises significant inconsistencies with the GDPR**, as well as with other Union law¹⁰, in particular as regards the following five aspects:
 - (a) Subject matter and scope of the Proposal
 - (b) Definitions/terminology used in the Proposal;
 - (c) Legal basis for the processing of personal data;

¹⁰ Although this observation does not strictly relate to the processing of personal data, the EDPB and the EDPS also notice possible confusion and ambiguities as to how the Proposal will apply together with the **Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union**. In this regard, it should be pointed out that the definitions of ‘processing’, ‘user’, ‘professional user’, and ‘data localization requirement’, as well as to other provisions of the Regulation on non-personal data (see for instance Article 6, *Porting of data*), might be not **consistent** or however overlapping with the definitions and the other provisions contained in the Proposal. Moreover, with regards to the re-use of data held by public sector bodies which are protected on grounds of statistical confidentiality, it should be pointed out that, despite the principle stated by Article 3(3) of the Proposal, the conditions for re-use defined in Article 5(3-4) are not in line with the sectoral rules established at EU level for the protection of confidential data used for statistical purposes (see Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities and the Commission Regulation (EU) No 557/2013 of 17 June 2013 implementing Regulation (EC) No 223/2009 of the European Parliament and of the Council on European Statistics as regards access to confidential data for scientific purposes and repealing Commission Regulation (EC) No 831/2002.

(d) Blurring of the distinction between (processing of) personal and non-personal data (and unclear relationship of the Proposal with the Regulation on free flows of non-personal data);

(e) Governance/tasks and powers of competent bodies and authorities to be designated in accordance with the Proposal, having regard to the tasks and powers of data protection authorities responsible for the protection of the fundamental rights and freedoms of natural persons in relation to the processing of personal data as well as for facilitating the free flow of personal data within the Union.

A. Subject matter and scope

26. According to Article 1(2) of the Proposal: “*This Regulation is without prejudice to specific provisions in other Union legal acts regarding access to or re-use of certain categories of data, or requirements relating to processing of personal or non-personal data.*”

Where a sector-specific Union legal act requires public sector bodies, providers of data sharing services or registered entities providing data altruism services to comply with specific additional technical, administrative or organisational requirements, including through an authorisation or certification regime, those provisions of that sector-specific Union legal act shall also apply.”

27. For the sake of clarity, the EDPB and the EDPS recommend introducing in Article 1 of the Proposal a provision clearly and unambiguously stating that the Proposal leaves intact and in no way affects the level of protection of individual with regard to the processing of personal data under the provisions of Union and national law and that the Proposal does not alter any obligations and rights set out in the data protection legislation. This addition would provide for better legal certainty and guarantees that fundamental right to the protection of personal data is not undermined.
28. In this regard it is unclear why a similar specification is contained in Article 9(2) of the Proposal referring to data sharing service providers¹¹ and not (*mutatis mutandis*, that is referring also to public sector bodies, re-users, data altruism organisations) as a horizontal provision under Article 1 of the Proposal.

B. The definitions of the Proposal are inconsistent with the definitions and key concepts of the GDPR, and therefore need to be amended or clarified

29. The definition of “*data holder*” provided under Article 2(5) of the Proposal: “the legal person or data subject who, in accordance with applicable Union or national law, has the right to grant access or to share certain personal or non-personal data under its control” is not in line with the overarching principles of the GDPR, as well as with the letter of the GDPR.
30. In this regard, the EDPB and the EDPS note that legal uncertainties may arise from the fact that the GDPR does not mention the data subject’s right to grant access or to share his/her personal data with

¹¹ Article 9(2) states: “*This Chapter shall be without prejudice to the application of other Union and national law to providers of data sharing services, including powers of supervisory authorities to ensure compliance with applicable law, in particular as regard the protection of personal data and competition law*”.

third parties and even less so an equivalent right for the legal person which seems possible to extrapolate from the definition of “data holder”. Rather, the GDPR guarantees to every individual the right to the protection of personal data concerning him or her, which refers to a comprehensive set of rules for the processing of personal data that are binding for each entity processing the data (data controller/joint controller) or processing the data on behalf of the data controller (processor)¹².

31. In this regard, the EDPS and the EDPB believe that rather than stating that a legal person has the right to grant access to or share personal data, it would be more appropriate referring to whether and under which conditions a certain processing of personal data can be performed or not.
32. A clarification that the EDPB and the EDPS would like to make is that both the access to and the sharing of personal data constitute processing of personal data pursuant to Article 4(2) of the GDPR.
33. According to the data protection legislation, the processing of personal data shall be lawful if the data subject (the identified or identifiable natural person to whom personal data relate) has given consent to the processing of his or her personal data for one or more specific purposes or if another adequate legal basis under Article 6 GDPR can be validly applied.
34. The aforesaid considerations are made in the light in particular of Article 8 of the Charter: “*1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.*”
35. The EDPB and the EDPS have concerns also as regards the wording of recital (14) of the Proposal (underline added): “*Companies and data subjects should be able to trust that the re-use of certain categories of protected data, which are held by the public sector, will take place in a manner that respects their rights and interests.*”; Article 11(6), referring to “*guarantees in place that allow data holders and data users to obtain access to their data in case of insolvency*”; as well as of Article 19, “*Specific requirements to safeguard rights and interests of data subjects and legal entities as regards their data*”, which refers under Article 19(1)(a) to: “*the purposes of general interest for which it [any entity entered in the register of recognised data altruism organisations] permits the processing of their data [of data holders] by a data user*”.
36. In this regard, the EDPB and the EDPS remark that rights and interests of the data subject with regard to his or her personal data, on the one hand, and the right and interests of legal persons with regard

¹² See also recital (6) and (7) of the GDPR (bold added):

“(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.”

to the information relating to them, on the other hand, are not of the same kind (the latter does not concern human dignity or the right to privacy and to data protection, but rather industrial property rights, such as trade secrets, patents and trademarks). Therefore, given the aforesaid heterogeneity, the mentioned provisions would be not only not conceptually ‘solid’, but also difficult to implement and such as to raise legal uncertainties. For instance, in case of insolvency (referred to under Article 11(6)), the guarantees in place to allow data holders to obtain access to non-personal data would differ substantially in practice from conditions and limits for the continued processing of personal data. These are indeed different issues that require different solutions¹³, and the reference to both under the obligation for the data sharing service provider to ensure continuity of provision of services (including the sharing of personal data) is confusing at least, if not manifestly inconsistent with the GDPR.

37. The definition of ‘data user’¹⁴ under Article 2(6) is also a new definition introduced by the Proposal, whose interplay -in case of personal data- with the definition of recipient¹⁵ under Article 4(9) of the GDPR is unclear. We note in this regard that Article 11(1) of the Proposal lays down: “The provider may not use the data for which it provides services for other purposes than to put them at the disposal of data users [...]” This provision, read in conjunction with the definition of ‘data user’, gives rise to legal uncertainty, due to different notions of ‘recipient’ under GDPR and ‘data user’ under the Proposal, which would lead to difficulties of practical application. Moreover, the definition under Article 2(6) might be misleading if read as referring to a natural or legal person that is authorised (has the right?) to use personal data for commercial and non-commercial purposes. The reference to and the meaning (its legal source and effect) of such “authorization” is also unclear.
38. In addition, the interplay between the notion of data user as “natural or legal person [authorised to use data for commercial and non-commercial purposes]” and the notions of controller, joint controller or processor under the GDPR is also unclear. Furthermore, the Proposal refers to a possible qualification as controller or processor and their obligations under the GDPR for the data sharing service providers¹⁶, but not for the data user or for the data altruism organisations (despite the fact that the latter can also be controller, joint controller or processor under the GDPR).
39. **More in general, the EDPB and the EDPS underline that the Proposal should define the roles in respect of personal data protection law (data controller, processor or joint controller) of each type of ‘actor’ (data sharing service provider, data altruism organisation, data user) not only to avoid**

¹³ For instance, in case of insolvency, attention should be paid to the fact that, as a result, there is a change in the controllership of the data processing. The new controller shall establish in particular what data can be processed; identify the purposes for which the data was originally obtained; establish the lawful basis for sharing the data; ensure compliance with the data protection principles, in particular lawfulness, fairness and transparency; inform data subjects about changes relating to the processing of their data, and consider that data subjects may exercise their right to object.

¹⁴ Article 2(6) of the Proposal: “**Data user** means a natural or legal person who has lawful access to certain data and is authorised to use that data for commercial or non-commercial purposes.”

¹⁵ According to the definition provided in the GDPR, under Article 4(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 [...].

¹⁶ See recital 28 “where the data sharing service providers are data controllers or processors in the sense of the Regulation (EU) 2016/679 they are bound by the rules of that Regulation.”

ambiguity about the applicable GDPR obligations, but also to improve the readability of the legal text.

40. Similar issues, namely the **unclear relationship with the definitions and rules provided under the GDPR**, relate to the definition of ‘data sharing’ under Article 2(7) of the Proposal (referring *inter alia* to the ‘joint or individual use of the shared data’). Insofar as it relates to personal data, the joint use of personal data (by both the data holder, legal person, and a data user) directly or through an intermediary, is also confusing at least.
41. Similar concerns - as further detailed below - relate to the term “permission [from legal entities to the reuse of data]”, for which however a definition is not provided in the Proposal.
42. The definition of ‘metadata’ in Article 2(4) is also problematic under the personal data protection viewpoint, since it refers to “data collected on any activity of a natural or legal person for the purposes of the provision of a data sharing service, including the date, time and geolocation data, duration of activity, connections to other natural or legal persons established by the person who uses the service”. Such data may include personal data.
43. As further detailed in this Joint Opinion, having regard to Article 11(2), the Proposal may be interpreted as creating a legal basis for the processing of metadata. Article 11 of the Proposal seems to lay down that, as a condition for providing the data sharing service, the provider should indeed be able to use the aforesaid metadata “for the development of that [the data sharing] service”. No reference is made in the legal text among others to the need for the data sharing service provider to rely upon an appropriate legal basis for processing of personal data under Article 6(1) of the GDPR.
44. **More in general, the EDPB and the EDPS consider that since the Proposal is, as made explicit in the Proposal itself, without prejudice to the GDPR, the definitions envisaged by the GDPR should apply and they should not be implicitly amended or removed by the Proposal and the new definitions, as far as they relate to the processing of personal data, should not, as ‘a matter of fact’, contain ‘rules’ that are inconsistent with the spirit and the letter of the GDPR.**
45. This specification is particularly important due to the cumulative effect in terms of lack of clarity and legal uncertainties arising from the Proposal where more than one unclear definition is contained in the same provision (see for instance Article 7(2)(c) of the Proposal, referring to “obtaining consent or permission by re-users for re-use for altruistic and other purposes in line with specific decisions of data holders”).
46. **In light of the above, the EDPB and the EDPS recommend clarifying and modifying the Proposal in order to ensure that -insofar as personal data are concerned- no inconsistencies with the definitions and concepts of the GDPR remain.**

C. The Proposal should better specify, to avoid legal uncertainties, the applicable legal basis in the GDPR for the processing of personal data

47. The EDPB and the EDPS notice that the Proposal makes reference to “the permission of data holders” for the use of data under several provisions:

- Article 5(6): “*the public sector body shall support re-users in seeking consent of the data subjects and/or permission from the legal entities whose rights and interests may be affected by such re-use*”, specified under recital (11): “*The public sector bodies, where relevant, should facilitate the re-use of data on the basis of consent of data subjects or permissions of legal persons on the re-use of data pertaining to them through adequate technical means.*”
 - Article 7(2)(c): “*assisting the public sector bodies, where relevant, in obtaining consent or permission by re-users for re-use for altruistic and other purposes in line with specific decisions of data holders [..]*”;
 - Article 11(11): “*where a provider provides tools for obtaining consent from data subjects or permissions to process data made available by legal persons*”;
 - Article 19(3): “*Where an entity entered in the register of recognised data altruism organisations provides tools for obtaining consent from data subjects or permissions to process data made available by legal persons*”, specified under recital (36) “*Legal persons could give permission to the processing of their non-personal data for a range of purposes not defined at the moment of giving the permission.*”
48. The EDPB and the EDPS notice in this regard that it is unclear in most cases whether the object of the permission would be the re-use of personal or non-personal data or both.
49. The EDPB and the EDPS also remark that in case of processing of personal data **the “permission” referred to in the Proposal cannot replace the necessity of one appropriate legal ground under Article 6(1) of the GDPR for the lawful processing of personal data**. In other words, according to the GDPR the processing of personal data shall be lawful only if and to the extent that at least one of the legal basis under Article 6(1) of the GDPR applies. The Proposal should clearly specify this aspect to avoid any ambiguity.
50. Indeed, even interpreting the notion of ‘permission’, (to be however defined in the legal text of the Proposal) as ‘a decision (a business choice) by a legal person to permit the processing of personal data where such legal person has a legal basis under Article 6(1) of the GDPR to permit such processing’, it has to be noted that the literal reading of some provisions of the Proposal does not seem to support this GDPR-compliant interpretation, since they refer for instance to “*Where the re-use of data cannot be granted in accordance with the obligations laid down in paragraphs 3 to 5 and there is no other legal basis for transmitting the data under Regulation (EU) 2016/679, the public sector body shall support re-users in seeking consent of the data subjects and/or permission from the legal entities*” (Article 5(6) of the Proposal)¹⁷. In these cases, ‘permission’ seems to be alternative to at least one (consent of the data subject) of the legal basis provided under Article 6 of the GDPR.
51. Recital 6 of the Proposal is also unclear with regard to the appropriate legal basis for the processing of personal data, since it refers to an obligation “in general” to rely on the legal basis provided in Article 6 of the GDPR for the processing of personal data¹⁸.

¹⁷ See also Article 7(2)(c); Article 11(11); Article 19(3) of the Proposal referred to above

¹⁸ In particular, recital 6 of the Proposals states that (bold added): “**In general**, insofar as personal data are concerned, the processing of personal data should rely upon one or more of the grounds for processing provided in Article 6 of Regulation (EU) 2016/679.”

52. From another standpoint, as a further detailed in this Opinion, the EDPB and the EDPS remark the need to **clarify the relationship between the different scenarios envisaged under the Proposal and Article 6(4) of the GDPR**, regulating the situation where the processing of personal data for a purpose other than that for which the personal data have been collected is not based on the data subject's consent.
53. **To that effect, in light of the objective and content of the Proposal, the EDPB and the EDPS consider that the Proposal cannot be invoked as Union law constituting a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1) of the GDPR in order to ground the processing for a purpose other than that for which the personal data has been initially collected, where such processing is not based on consent, as per Article 6(4) of the GDPR.**
54. **Also in light of the above, the EDPB and the EDPS recommend specifying in the legal text of the Proposal that insofar as personal data are concerned, their processing must always be based on an adequate legal basis under Article 6 of the GDPR.**
55. As an example of possible inconsistency relating to the legal basis for the processing of personal data, we point out to the provision under Article 11(2) of the Proposal, according to which "*the metadata collected on the basis of the data sharing offered may be used [only] for the development of the data sharing services*". In this regard, we recall that metadata referred to in the Proposal¹⁹ can constitute information relating to an identified or identifiable natural person and in this case must be processed in accordance with data protection rules and, in particular, those concerning the legal basis of the processing. However, as referred to in paragraph 51 of this Opinion, this essential aspect is not addressed by the Proposal.
56. **On this matter, as a broader observation, the EDPB and the EDPS consider that the aforesaid provision, as well as any other provision of the Proposal, does not provide a self-standing legal basis for the re-use of personal data by data users and for the processing activities performed by providers of data sharing services or by data altruism organisations, due to the fact that it does not fulfil the criteria under Article 6(3) for the processing referred to in point (c) and (e) of Article 6(1)²⁰ of the GDPR.**

¹⁹ Under Article 2(4) of the Proposal “‘metadata’ means data collected on any activity of a natural or legal person for the purposes of the provision of a data sharing service, including the date, time and geolocation data, duration of activity, connections to other natural or legal persons established by the person who uses the service.”

²⁰ “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

D. Blurring of the distinction between (processing of) personal and non-personal data and unclear relationship of the Proposal with the Regulation on free flows of non-personal data

57. As a general remark, the EDPB and the EDPS consider that a main criticality of the Proposal, having regard to the protection of personal data, possibly at the origin of the aforesaid incompatibilities or at least ambiguity of the legal text, is the blurring of the distinction between the processing of non-personal data, as regulated for certain aspects under Regulation (EU) 2018/1807 of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (“Regulation on the free flow of non-personal data”)²¹, and the processing of personal data, the latter regulated under the data protection acquis and inspired by different principles.
58. In this regard, the EDPB and the EDPS underline that the distinction between categories of personal and non-personal data is difficult to apply in practice. Indeed, in practice, from a combination of non-personal data it is possible to infer or generate personal data, i.e. data relating to an identified or identifiable individual²², especially when non-personal data are the result of the anonymisation of personal data and thus information originally related to natural persons. In addition, in the scenarios envisaged by the Proposal of increased availability, re-use and sharing of information, with a view to “allowing ‘Big Data’ pattern detection or machine learning”²³, the more non-personal data are combined with other available information, the more difficult it will be to ensure anonymisation because of the increased re-identification risk for data subjects. Consequently, having this scenario in mind, the data subjects’ fundamental rights to privacy and data protection should be ensured in any case in the different contexts envisaged by the Proposal.
59. At the same time, there might be cases of non-personal data, to which the GDPR does not apply, that since their origin, do not relate to natural persons. For instance, it is the case of non-personal data from vibration sensors in industrial machinery combined with other non-personal data, e.g. the geolocation of the machinery. Such non-personal data does not need the same level of safeguards than non-personal data that are the result of the anonymisation of personal data, as only the latter (likewise pseudonymised data) are likely to be exposed to the risk of re-identification.
60. **To avoid confusion as to how the Proposal would apply ‘together with the GDPR’, the EDPB and the EDPS recommend reworking the Proposal taking better into account the distinction between personal and non-personal data as well among different types of non-personal data.**

Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.”

²¹ Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance.), OJ L 303, 28.11.2018, p. 59–68.

²² See EDPS Opinion 3/2020 on the European strategy for data at para 30.

²³ Explanatory Memorandum, page 3.

61. Therefore, notwithstanding the concerns already expressed by the EDPS with regard to the concept of mixed dataset and to “inextricably linked” personal and non-personal data²⁴, the EDPB and the EDPS recall that, according to Article 2(2) of the Regulation on the free flow of non-personal data: *“In the case of a data set composed of both personal and non-personal data, this Regulation applies to the non-personal data part of the data set. Where personal and non-personal data in a data set are inextricably linked, this Regulation shall not prejudice the application of Regulation (EU) 2016/679.”* Consequently, a mixed dataset will as a rule be subject to the obligations of data controllers and processors and the data subject’s rights established by the GDPR. This consideration is particularly relevant in the context of the Proposal, since it is possible that in most cases datasets shared through a data sharing service provider or a data altruism organisation would also contain personal data. Since a ‘third category’ between personal and non-personal data does not exist, this would not change the nature and the ‘legal regime’ of the dataset as personal data²⁵.
62. **In the light of the above, the EDPB and the EDPS point out to the risk that the Proposal creates a parallel set of rules, which are not consistent with the GDPR, nor with the Regulation on the free flow of non-personal data, thus undermining it and causing difficulties of practical application.**

E. Governance/tasks and powers of competent bodies and authorities to be designated in accordance with the Proposal and tasks and powers of the data protection authorities

63. The Proposal foresees the designation by Member States of competent bodies to support the public sector bodies which grant access to the re-use of data (Chapter II of the Proposal) and the designation of competent authorities to monitor the compliance with the provisions related to data sharing services and data altruism (Chapters III and IV of the Proposal).
64. **As a broader remark, the EDPB and the EDPS are of the opinion that, since many of the tasks of the competent bodies and authorities under the Proposal relate to the processing of personal data, there is a risk of interferences by the competent bodies and authorities designated under the Proposal with the competence and tasks of independent data protection authorities. Therefore, the designation of competent authorities/bodies other than data protection authorities could lead to real complexity for digital players and data subjects, and also affect consistency in terms of monitoring the application of the provisions of the GDPR. The designation of competent bodies and authorities being left at the discretion of Member States, there may also be a risk of inconsistency and divergence in regulatory approaches across the Union.**

²⁴ See the Comments of the EDPS on a Proposal for a Regulation of the European Parliament and of the Council on a framework for the free-flow of non-personal data in the European Union issued on the 8th June 2018 at https://edps.europa.eu/sites/edp/files/publication/18-06-08-edps_formal_comments_freeflow_non_personal_data_en.pdf.

²⁵ See also Communication from the Commission to the Council and to the European Parliament, *Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, at: <https://ec.europa.eu/digital-single-market/en/news/guidance-regulation-framework-free-flow-non-personal-data-european-union>

3.3 Re-use of certain categories of protected data held by public sector bodies

3.3.1 Relationship of the Proposal with the Open Data Directive and with the GDPR

65. While the Explanatory Memorandum states that the Proposal “*complements the Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (Open Data Directive)*²⁶”, recital (5) further specifies that “*Directive (EU) 2019/1024 as well as sector-specific legislation ensure that the public sector makes more of the data it produces easily available for use and re-use. However, certain categories of data (commercially confidential data, data subject to statistical confidentiality, data protected by intellectual property rights of third parties, including trade secrets and personal data not accessible on the basis of specific national or Union legislation, such as Regulation (EU) 2016/679 and Directive (EU) 2016/680) in public databases is often not made available, not even for research or innovative activities. Due to the sensitivity of this data, certain technical and legal procedural requirements must be met before they are made available, in order to ensure the respect of rights others have over such data. Such requirements are usually time- and knowledge-intensive to fulfil. This has led to the underutilisation of such data. While some Member States are setting up structures, processes and sometimes legislate to facilitate this type of re-use, this is not the case across the Union.*”
66. The EDPB and the EDPS observe that, despite the aforesaid specifications, the interface of the Proposal with the “Open Data Directive” seems unclear. In particular, there might be legal uncertainty on the extended re-use of public sector information, which, according to Article 3 (Categories of data) of the Proposal, would apply to:
- “[...]data held by public sector bodies which are protected on grounds of:
- (a) commercial confidentiality;
 - (b) statistical confidentiality;
 - (c) protection of intellectual property rights of third parties;
 - (d) protection of personal data.”
67. The Explanatory Memorandum to the Proposal²⁷ does not sufficiently clarify the scope of such extended re-use and the interplay of the Proposal with the Open Data Directive. Moreover, it puts under the same ‘umbrella’ (as “*respect of rights of others*”), which is inappropriate having regard to

²⁶ OJ L 172, 26.6.2019, p. 56–83.

²⁷ See at page 7: “*Chapter II creates a mechanism for re-using certain categories of protected public sector data, which is conditional on the respect of rights of others* (notably on grounds of protection of personal data, but also protection of intellectual property rights and commercial confidentiality). *This mechanism is without prejudice to sector-specific EU legislation on access to and the re-use of this data. The re-use of such data falls outside the scope of Directive (EU) 2019/1024 (Open Data Directive). Provisions under this Chapter do not create right to re-use such data, but provide for a set of harmonized basic conditions under which the reuse of such data may be allowed (e.g. the requirement of non-exclusivity).*”

the protection of personal data) “protection of personal data, but also protection of intellectual property rights and commercial confidentiality”.

68. It can be argued that the wording “*data held by public sector bodies which are protected on the grounds of*”, among others “protection of personal data” (Article 3, letter (d)) is at the same time:
- regrettable, since it suggests the idea of data protection regulation as *impeding* the free movement of personal data, rather than laying down the rules of free flow of personal data while protecting the rights and interests of the persons concerned; *and*
 - partially inaccurate, since the Open Data Directive, rather than excluding personal data from its scope²⁸, provides, under Article 1(2)(h), that [the Open Data Directive does not apply to] “*documents, access to which is excluded or restricted by virtue of the access regimes on grounds of protection of personal data, and parts of documents accessible by virtue of those regimes which contain personal data the re-use of which has been defined by law as being incompatible with the law concerning the protection of individuals with regard to the processing of personal data or as undermining the protection of privacy and the integrity of the individual, in particular in accordance with Union or national law regarding the protection of personal data*”²⁹.
69. This last aspect is however specified under recital 7 of the Proposal³⁰. In this regard, the EDPB and the EDPS wonder why this important issue (as well as many others concerning the protection of personal data) is included in a recital, but not in the substantive part of the Proposal.
70. Moreover, pursuant to Article 3(1) of the Open Data Directive, personal data that do not fall under this exception, being freely accessible according to the Union or national access regimes and re-usable for compatible uses without undermining the protection of privacy and the integrity of the individual, are within the scope of the Directive and can be made available for re-use in accordance to the conditions set out in the same Directive as well as in compliance to the requirements of data protection law . Indeed, as stated in recital 154 of the GDPR, the EU legislation on the re-use of public sector information “*leaves intact and in no way affects the level of protection of natural persons with regard to the processing of personal data under the provisions of Union and Member State law, and in particular does not alter the obligations and rights set out in [the GDPR]*”. To this effect, the EU legislator when establishing new principles and rules for the re-use of public sector information should provide for the necessary reconciliation of such re-use with the right to the protection of personal data pursuant to the GDPR³¹.
71. **Consequently, the EDPB and the EDPS underline that the rules of the Open Data Directive along with those of the GDPR provide already for mechanisms allowing the sharing of personal data held by**

²⁸ See Article 1 of the Open Data Directive.

²⁹ See also in this regard, recital 52 and 53 as well as Articles 1(4) and 10 of the Open Data Directive, the latter with specific reference to research data.

³⁰ “*The data covered by this Regulation fall outside the scope of Directive (EU) 2019/1024 that excludes data subject to commercial and statistical confidentiality and data for which third parties have intellectual property rights. Personal data fall outside scope of Directive (EU) 2019/1024 insofar as the access regime excludes or restricts access to such data for reasons of privacy and the integrity of the individual, in particular in accordance with data protection rules.*” (emphasis added).

³¹ See recital 154 as well as Article 86 of the GDPR with specific reference to Union and Member State law on public access to official documents

the public sector bodies in a manner consistent with the requirements governing protection of individuals' fundamental rights. Thus, the EDPB and the EDPS recommend to align Chapter II of the Proposal with the existing rules on the protection of personal data laid down in the GDPR and with the Open Data Directive, so as to ensure that the level of personal data protection in the EU is not undermined and to avoid, at the same time, that these misalignments generate legal uncertainty for individuals, public sector bodies and re-users. As an alternative, without prejudice to the further indications in this Joint Opinion about the impact on the individuals' right to privacy and data protection of the rules of the Proposal governing the re-use of certain categories of protected data held by public sector bodies, personal data could be excluded from its scope.

[3.3.2 Article 5: conditions for re-use of data by public sector bodies](#)

72. The conditions for re-use of data held by public sector bodies are provided under Article 5 of the Proposal as specified under recital 11. In this regard, the EDPB and the EDPS consider that the Proposal raises some concerns.
73. **The EDPB and the EDPS reiterate that all processing of personal data as referred to in the Proposal shall occur in full compliance with the GDPR, and thus accompanied by appropriate data protection safeguards. This means that the re-use of personal data should always respect the principles of lawfulness, fairness and transparency as well as purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality in line with Article 5 of the GDPR.**
74. In this scenario, fairness, transparency and purpose limitation are essential safeguards to bring trust among individuals whose personal data are held by the public sector, making them confident that the re-use of the information they provide will take place in a manner that respects their rights and interests (see recital 14 of the Proposal), i.e., that their personal data will not be used against them in an unexpected manner. The importance of the principle of purpose limitation is clearly demonstrated in the context of the measures that are being considered to fight against the COVID-19, e.g. health data to be processed under the control of healthcare authorities as data controllers and not to be used for commercial or other incompatible purpose³². Consequently, public sector bodies which are competent under national or EU law to grant or refuse access for the re-use must take into account that the re-use of personal data is permissible only if the principle of purpose limitation as set out in point (b) of Article 5(1) and Article 6 of the GDPR is met³³. Any subsequent use of data, collected and/or shared in pursuit of a public task (e.g. for improving transport/mobility or tackling serious cross-border threats to health), for commercial for-profit purposes (for instance insurance, marketing, etc.) should be avoided. Such "function creep" might not only constitute a breach of the data protection principles under Article 5 of the GDPR, but could also undermine the trust of individuals in the re-use mechanism, which is a fundamental aim of the Proposal (see recitals 14 and 19)³⁴.
75. In this regard, the EDPB and the EDPS recall that Article 6(4) GDPR clarifies the concept of 'compatible further processing' (of personal data). Indeed, according to the definition of 're-use' set out in Article 2(2) of the Proposal, when it concerns personal data, the re-use is to be regarded, under a data protection perspective, as a further processing of personal data held by public sector bodies for

³² See EDPS Opinion on the European Strategy for Data, paragraph 10.

³³ See in this regard recital (52) of the Open Data Directive.

³⁴ See EDPS Opinion on the European Strategy for Data, paragraph 25.

subsequent not well described (commercial or non-commercial) purposes. However, Article 5 of the Proposal, concerning the conditions for re-use, does not provide any indication on the purposes for which the re-use may be lawfully authorised, nor it specifies that the purposes of any subsequent re-use have to be carefully identified and clearly defined in Union or Member State law in compliance with Article 6(1)(c) or 6(1)(e) and 6(3) of the GDPR³⁵, eventually satisfying the requirements of Article 23(1) of the GDPR pursuant to Article 6(4) of the GDPR³⁶.

76. More generally, the Proposal does not seem to lay down any legal obligation for public sector bodies to make data they held available for re-use, nor does it explicitly aim at safeguarding the objectives listed in Article 23 of the GDPR.
77. **Therefore, the EDPB and EDPS strongly recommend to amend the Proposal so as to clarify that the re-use of personal data held by public sector bodies may only be allowed if it is grounded in Union or Member State law which lays down a list of clear compatible purposes for which the further processing may be lawfully authorised or constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23 of the GDPR.**
78. **Furthermore and in line with the above recommendation, to allow a lawful access to personal data by “data users”, as indicated by the definition of ‘data users’ pursuant to Article 2(6) of the Proposal, public sector bodies, which are competent under national or EU law to grant or refuse such access for the re-use, must rely on an adequate legal basis under Article 6 of the GDPR being applicable to the said disclosure. However, this aspect is not specified under Article 5 of the Proposal referring to the conditions for re-use of personal data held by public sector bodies.**
79. Indeed, recital 11 of the Proposal and the corresponding Article 5(3)-(6) does not refer to Union or Member State law that would provide the legal basis under Article 6(1)(c) or (e) of the GDPR, but lays down (bold added): “*In particular, personal data should only be transmitted for re-use to a third party where a legal basis allows such transmission*”. In this respect, it shall be noted that the reference should be to the legal basis “under the GDPR”. Moreover, the said recital restricts itself to state that “[t]he public sector bodies, where relevant, should facilitate the re-use of data on the basis of consent of data subjects or permissions of legal persons on the re-use of data pertaining to them through adequate technical means. In this respect, the public sector body should support potential re-users in seeking such consent by establishing technical mechanisms that permit transmitting requests for

³⁵ According to Article 6.3 GDPR, Union or Member State law under Article 6(1)(c) or 6(1)(e) of the GDPR should identify amongst other elements the “purpose limitation” of the personal data processing as well as the “purpose for which data may be disclosed”.

³⁶ In another respect, the inclusion of data held by public sector bodies which are protected on grounds of statistical confidentiality in the scope of Chapter II of the Proposal, according to its Article 3(1)(b) and despite the principle stated in its Article 3(3), risks to contradict, the essential principles of data protection in the statistical sector and in particular, the purpose limitation principle, which strictly prohibits the use of confidential data for purposes that are not exclusively statistical, thus undermining trust of natural persons in providing their personal data for statistical purposes (see recital 27 of the above mentioned Regulation (EC) No 223/2009 on European statistics and Articles 4(1) and 4(2) of the Recommendation of the Council of Europe No R (97)18 concerning the protection of personal data collected and processed for statistical purposes).

consent from re-users, where practically feasible. No contact information should be given that allows re-users to contact data subjects or companies directly."

80. The wording of recital 14 of the Proposal is also unclear in setting out the interplay of this Chapter of the Proposal with the GDPR: "[...] Additional safeguards should thus be put in place for situations in which the re-use of such public sector data is taking place on the basis of a processing of the data outside the public sector. Such an additional safeguard could be found in the requirement that public sector bodies should take fully into account the rights and interests of natural and legal persons (in particular the protection of personal data, commercially sensitive data and the protection of intellectual property rights) in case such data is transferred to third countries"³⁷.
81. Furthermore, the EDPB and the EDPS notice that Article 5(6) of the Proposal lays down "Where the re-use of data cannot be granted in accordance with the obligations laid down in paragraphs 3 to 5 and there is no other legal basis for transmitting the data under Regulation (EU) 2016/679 [...]" . In this regard, the EDPB and the EDPS are of the opinion that the conditions listed under paragraphs 3 to 5 (among which, access and re-use of data within a secure processing environment) cannot be considered as an alternative to the legal basis exhaustively listed under Article 6 of the GDPR, unless the reference to (Union or) Member State law is made in the aforesaid paragraphs³⁸.
82. In addition, it is unclear the role of the public sector body in supporting re-users in obtaining the consent for the reuse by the data subject. As a further remark on Article 5(6) of the Proposal, the EDPB and the EDPS point out that this provision establishes an obligation for public sector bodies ("shall support"), whose content is not well defined. More to the point, the legal basis under the GDPR for contacting data subjects to collect their consent for the re-use should be specified, as well as the respective responsibility related to obtaining a valid consent under Article 7 of the GDPR.³⁹ In this regard, it should also be taken into account the clear imbalance of power which is often present in the relationship between the data subject and the public authorities⁴⁰. In this context, in line with the GDPR accountability principle, the EDPB and the EDPS recall that the choice of an appropriate legal basis for the processing of personal data, as well as the demonstration that the chosen legal basis (in this case consent) can be validly applied, lies on the data controller.
83. Therefore, in line with the principle of lawfulness established by the GDPR, the EDPB and EDPS strongly recommend to clarify, among the conditions for re-use provided for in Article 5 of the Proposal, that an appropriate legal ground under GDPR must be provided in Union or Member State law and carefully identified by public sector bodies with regard to any subsequent re-use of personal data.

³⁷ In addition, the EDPB and EDPS note that public sector bodies should not just take into account but **comply with** the legal framework protecting the rights and interests of data subjects.

³⁸ It might also be worth specifying, for the sake of clarity, that intellectual property rights, referred to under Article 5(7), do not allow (constitute a legal basis for) the processing of personal data.

³⁹ Would it be the responsibility of the public sector body or of the re-user?

⁴⁰ In another respect, it should be reminded that consent in most cases is not an appropriate legal basis for the processing activities performed by public authorities. See the EDPB Guidelines 5/2020 on consent under Regulation 2016/579 at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

84. Other key elements to build the level of trust aimed at in the Proposal are the fairness and the transparency principles. According to these principles, individuals must be fully aware whether the personal data they provide to the public sector bodies, or that are further processed by the same bodies in the pursuit of their public tasks, will become subject to re-use and for which purposes, as well as the recipients or categories of recipients to whom the personal data will be disclosed taking into account that in most cases data subjects are compelled under national law to provide their personal data to public bodies because of legal obligations or because they apply for a public action or service⁴¹.
85. However, among the conditions for re-use established in Article 5 of the Proposal, there is no reference to the obligations for the public sector bodies of informing the data subjects under the GDPR, nor to the need of involving them in the process of enabling the re-use of their personal data. This not only undermines the principles of fairness and transparency established by the GDPR to ensure that individuals have a clear overview and control on the possible uses of their own personal data, but also contradicts the same goals of the Proposal which is to increase trust of data subjects that the re-use “will take place in a manner that respects their right and interests” ⁴². **Therefore, the EDPB and EDPS recommend to include in the Proposal an explicit reference to the obligations for the public sector bodies of informing the data subjects under the GDPR so that to foster the exercise of the rights conferred to them by the data protection legislation, especially the right to object pursuant to Article 21 of the GDPR. In this respect, the EDPB and EDPS also recommend to define in the Proposal adequate means by which individuals may participate, in an open and collaborative manner, in the process of allowing the re-use of their personal data.**
86. Moreover, to attain a reasonable level of trust in the re-use mechanism, public sector bodies, competent under national or EU law to allow access for the re-use must respect the principles of data minimisation and consider the special protection required for specific sectors routinely dealing with special categories of personal data, such as the health sector, when they establish the scope and conditions for allowing access for the re-use. In assuming these decisions, accuracy, storage limitation, integrity and confidentiality of personal data should also be carefully considered, as well as the potential impact on the concerned data subjects.
87. **In this regard, the EDPB and EDPS call the attention of the legislator to the need of addressing the necessary requirements of the protection of personal data, especially in “sensitive sectors” such as the health sector, when establishing the rules governing the re-use of personal data, as well as the related conditions and specific data protection safeguards.**
88. In particular, according to the GDPR, the data protection impact assessment (DPIA) is a key tool to ensure that data protection requirements are properly taken into account and the rights and interests of individuals are adequately protected, so as to foster their trust in the re-use mechanism. Therefore, the EDPB and EDPS recommend to include in the text of the Proposal that a DPIA must be performed by public sector bodies in case of data processing falling under Article 35 of the GDPR⁴³. The DPIA will help to identify the risks and the appropriate data protection safeguards for the re-use addressing

⁴¹ See Court of Justice of the European Union, C-201/14, *Smaranda Bara and Others*, 1 October 2015, ECLI:EU:C:2015:638.

⁴² See Recital 14 of the Proposal

⁴³ See in this regard recital (53) of the Open Data Directive.

those risks, in particular for specific sectors routinely dealing with special categories of personal data. The decision on the re-use, in addition to being grounded on Union or Member State law, especially for some “sensitive sectors” (health sector, but also transport or energy grids) should be based on this assessment, as well as the specific conditions for the re-users and the concrete safeguards for data subjects(for example, clarifying the risks of re-identification of anonymised data and the safeguards against those risks). Finally, the results of such assessment, whenever possible, should be made public, as a further measure enhancing trust and transparency⁴⁴.

89. As for the conditions for re-use, Article 5(3) of the Proposal specifies that public sector bodies “may” impose an obligation to re-use only prior anonymized or pseudonymised personal data. This means that public sector bodies are not obliged to pre-process personal data so that to make available to re-users only prior anonymized or pseudonymised personal data. Consequently, public sector bodies may disclose to re-users even data which allow the natural persons - to whom the data relate - to be directly identified, if provision of anonymised data “would not respond to the needs of the re-user” ⁴⁵. In this case, on-premise or remote re-use of personal data within a secure processing environment could still be permitted by public sector bodies under Article 5(4) of the Proposal. However, given the rapid developments in re-identification techniques and the availability of advanced computational resources, the legislator should take into account that anonymisation, pseudonymisation, and even the use of secure environments cannot be considered in all cases as free from vulnerabilities, especially in the long term.
90. In this context, the EDPB and the EDPS welcome that recital 11 of the Proposal envisages that “the use of such secure processing environment” may be made by the public sector body *“conditional on the signature by the re-user of a confidentiality agreement that prohibits the disclosure of any information that jeopardises the rights and interests of third parties that the re-user may have acquired despite the safeguards put in place”*. However, the EDPB and the EDPS also recommend to include a reference to such confidentiality agreement in the legal text of the Proposal among the conditions for re-use laid down in Article 5. This agreement should also prohibit the re-users from re-identifying any individual to whom the data relates and should contain the obligation for the re-users to assess on an on-going basis the risks of re-identification and to report any data breach resulting in the re-identification of the individuals concerned not only to the Data Protection Authority and the data subjects pursuant to Articles 33 and 34 of the GDPR, but also to the public sector body concerned.
91. In any case, the EDPB and EDPS emphasize that anonymisation and pseudonymisation cannot be placed at the same level and should be weighted differently by public sector bodies in assessing the re-use from a data protection perspective. Indeed, anonymisation represents a means of fostering the public sector information re-use in a pro-competitive perspective, while also meeting the various requirements under data protection legislation, given that ‘anonymous information’, as defined in Recital 26 of the GDPR, does not fall within the scope of the said legislation. On the contrary, information which has undergone pseudonymisation (which could lead to re-identification by a natural person by the use of additional information) should still be considered “personal data”, thus entailing the application of other measures required by the data protection legislation, while

⁴⁴ See EDPS Opinion on the proposal for a recast of the Public Sector Information (PSI) re-use Directive, available at: https://edps.europa.eu/sites/edp/files/publication/18-07-11_psi_directive_opinion_en.pdf

⁴⁵ See recital 11 of the Proposal

reducing the risks for data subjects and helping public sector bodies and re-users to meet data protection obligations (in particular the principles of data protection by design and by default and data minimisation). The latter considerations apply also to the measures envisaged by Article 5(4) of the Proposal that public sector bodies may impose as conditions for re-use.

3.3.3 Article 5(11): re-use of “highly sensitive” non-personal data

92. Article 5(11) introduces the concept of non-personal data that have been identified as “highly sensitive”, as regards the transfer to third countries, by Union law. Recital 19 of the Proposal provides some examples: “in the health domain, certain datasets held by actors in the public health system, such as public hospitals” “identified as highly sensitive health data”, “for example in the context of the European Health Data Space or other sectoral legislation”. With regard to such non-personal data, the Commission shall adopt delegated acts laying down special conditions applicable to the transfer of such data to third countries.
93. In this regard, the EDPB and the EDPS note that even if information in a anonymised data set does not present a risk of directly identifying or singling out a natural person, when this information is combined with other available information, it could entail the risk of indirect identification, so that it is likely to fall within the scope of the definition of personal data. Indeed, the more information is available and data are re-used and shared, the more difficult it will be to ensure anonymisation over time.⁴⁶ Consequently, the EDPS and the EDPB would like to draw attention to the fact that much of the data already today -and increasingly in the future- generated and processed by techniques of artificial intelligence, machine learning, internet of things, cloud computing and big data analysis, are often likely to fall within the scope of the definition of personal data. In this scenario, **the EDPB and the EDPS calls upon the legislator to consider that even the re-use of non-personal “highly sensitive” data envisaged by the Proposal may have an impact on the protection of personal data, especially if such non-personal data are the result of the anonymisation of personal data and thus information originally related to individuals.** Indeed also in these cases, the data subjects’ fundamental rights to privacy and data protection must be fully ensured. Moreover, the EDPB and the EDPS strongly recommend clarifying the concept of “highly sensitive non-personal data”, as a minimum by providing concrete examples.

3.3.4 Article 6: fees for data re-use

94. As for the fees envisaged under Article 6 of the Proposal, the EDPB and the EDPS note that the Open Data Directive contains an explicit reference to ‘anonymisation costs’ in Recitals 36 and 38 as well as in Article 6, paragraphs (1), (4) and (5). In particular, the Open Data Directive provides for an exception to the re-use of documents free of charge in order to allow public sector bodies to charge re-users the reasonable expenses they incur in to pre-process, aggregate and/or anonymise the personal data

⁴⁶ See in this regard, the WP29 Opinion 05/2014 on Anonymisation techniques (WP 216) as well as the Judgment of the ECJ of 19 October 2016, Patrick Breyer v Bundesrepublik Deutschland, in case C-582/14 which refers to Recital 26 of Directive 95/46/EC, looking at the legal and practical means by which re-identification may be affected by the use of additional data in the hands of third parties. The forthcoming EDPB guidelines on anonymisation/pseudonymisation will further elaborate upon this matter.

offered for re-use, in situations where the use of such techniques would be justified in light of the increased risks deriving from offering such data for re-use.

95. Given that, in certain cases, the pseudonymisation or anonymisation of information held by public sector bodies can be a complex, time-consuming and expensive task requiring expertise that might not always be available, the EDPB and the EDPS recommend including in Article 6(5) of the Proposal that **fees charged by public sector bodies for allowing the re-use of data may duly take into account the costs incurred by public sector bodies for the pseudonymisation or anonymisation** of personal data made available for reuse.
96. It can also be noted that **the Proposal reverses the general principle established by the Open Data Directive of “free of charge” re-use.** Indeed, Article 6(1) of the Proposal states that “*public sector bodies which allow re-use of the categories of data referred to in Article 3 (1) may charge fees for allowing the re-use of such data.*” In this regard, the interplay with the Open Data Directive is therefore unclear.
97. Moreover, it can be observed that, even though Article 6(5) specifies that “Fees shall be derived from the costs related to the processing of the requests for re-use (...), the Proposal seems to introduce financial incentives to public sector bodies to allow the re-use of personal data.
98. It also has to be noted that Article 6(4) imposes an obligation to public sector bodies to “*take measures to incentivize the reuse of the categories of data referred to in Article 3 (1) [which include personal data] for non-commercial purposes and by small and medium-sized enterprises in line with State aid rules.*”
99. This aspect, also in the light of the criticalities of the Proposal described in the general comments of this Joint Opinion, is problematic from a data protection viewpoint, under both legal and practical implementation’s perspective. In particular, the lack of clarity on the type of incentives and addressees thereof may raise additional questions as to whether consent, as one of the legal basis relied upon under Article 5(6) of the Proposal for the re-use personal data, will be the appropriate legal ground, especially with regard to the individuals’ freedom of choice to refuse to provide their consent to the re-use of their personal data or to withdraw it⁴⁷.

3.3.5 Governance and institutional aspects: Article 7 (competent bodies). Article 8 (single information point).

100. The Proposal provides that Members States will have to set up a single contact point for reuse of public sector data (Article 8), and to establish bodies in charge of supporting public sector bodies with technical means and legal assistance for reuse of public sector data (Article 7). Pursuant to Article 7(3), such “competent bodies” may be entrusted to grant access for the reuse of data, including personal data.

⁴⁷ As stated in the EDPB Guidelines 05/2020 on consent under GDPR, in general terms, any element of inappropriate pressure or influence upon the data subject (which may be manifested in many different ways) which prevents a data subject from exercising their free will, shall render the consent invalid.

101. Therefore, with regard to the competent bodies, they will, inter alia, assist the public sector bodies in obtaining consent or permission for the re-use and can also be entrusted to grant access for the re-use of data held by the public sector body, including personal data.
102. Firstly, the provision under Article 7(2)(c) should be clarified, due in particular to the vagueness of the terminology used (“permission by re-users for reuse”; “altruistic and other purposes”; “in line with specific decisions of data holders”). The overall meaning of the provision (“the competent bodies assist the public sector bodies, where relevant, in obtaining consent or permission *by re-users for re-use* for altruistic and other purposes in line with specific decisions of data holders”) is therefore also unclear.
103. Secondly, despite those bodies are essentially tasked with support and advisory duties vis-à-vis public sector bodies for data re-use, some of their tasks deal with implementing the safeguards set out in the data protection legislation and fostering the protection of the rights and interests of individuals with regards to their personal data. However, Chapter II of the Proposal does not clarify whether data protection supervisory authorities - to which the GDPR also confers, among others, advisory powers - may be designated as the competent body under Article 7 of the Proposal⁴⁸.
104. In this regard, the EDPS and the EDPB firstly underline that the designation and multiplication of competent bodies that may deal, to some extent, with personal data processing under Chapter II of the Proposal could lead to real complexity for public sector bodies, re-users and data subjects, and also affect consistency in terms of monitoring the application of the provisions of the GDPR. **Hence, inasmuch as personal data is being subject to re-use on the basis of the Proposal, the EDPB and the EDPS consider that the data protection supervisory authorities should be the only ones competent for the oversight of such personal data processing. Adequate resources should be provided to these authorities to allow them to effectively and efficiently perform this task.**
105. **Furthermore, should specific bodies be designated to assist public sector bodies and data re-users and be entrusted to grant access for the reuse of data, including personal data, such bodies may not be referred as “competent” as they would not act as a supervisory authority able to monitor and enforce the provisions related to the processing of personal data. In order to ensure legal certainty and consistency of the application of the EU acquis in the field of personal data protection, the activities and obligations of such designated bodies shall also be subject to the direct competence and supervision of data protection authorities, when personal data is involved.**
106. **As per their competence and tasks under the GDPR, data protection authorities have already specific expertise in the monitoring of the compliance of data processing, as well as in promoting awareness of controller and processor of their obligation related to the processing of personal data. Therefore, in order to ensure consistency between the institutional framework envisaged by Chapter II of the Proposal and the GDPR, the EDPB and the EDPS recommend to clarify that the main competent authorities for the supervision and enforcement of the provisions of Chapter II related to the processing of personal are the data protection supervisory authorities. The latter authorities should**

⁴⁸ As it is the case, for example, in the context of existing data spaces, such as the French Health Data Hub, where the FR data protection authority is the one competent to authorise access to specific personal data. See also in this regard the advisory powers conferred to the data protection authorities in the context of a DPIA, in order ensure their compliance with the rules for the protection of personal data according to Articles 57(1)(l) and 58(3)(a) of the GDPR.

work closely with the specific bodies designated, under the Proposal, to assist public sector bodies and re-users and entrusted to grant access for the reuse of data, in consultation with other relevant sectorial authorities, when necessary, so as to ensure a coherent application of these provisions.

107. The EDPB and the EDPS also observe that the Proposal does envisage under Article 8(4) a mechanism for redress for re-users where they wish to challenge the decision of refusing access for re-use that is different from the one established under the Open Data Directive. Under the Open Data Directive (See Article 4(4)), in particular, the means of redress shall include the possibility of review by an impartial review body with the appropriate expertise, such as, among others, “*the supervisory authority established in accordance with Regulation (EU) 2016/679 or a national judicial authority, whose decisions are binding upon the public sector body concerned*”. In this respect, without prejudice to the observations already made in this Joint Opinion on the need of clarifying the interplay of the Proposal with the Open Data Directive, the EDPB and the EDPS call the attention of the legislator on the inconsistencies between those two set of rules.

3.4 Requirements applicable to data sharing service providers

The Explanatory Memorandum illustrates that “*Chapter III aims to increase trust in sharing personal and non-personal data and lower transaction costs linked to B2B and C2B data sharing by creating a notification regime for data sharing providers. These providers will have to comply with a number of requirements, in particular the requirement to remain neutral as regards the data exchanged. They cannot use such data for other purposes. In the case of providers of data sharing services offering services for natural persons, the additional criterion of assuming fiduciary duties towards the individuals using them will also have to be met. The approach is designed to ensure that data sharing services function in an open and collaborative manner, while empowering natural and legal persons by giving them a better overview of and control over their data. A competent authority designated by the Member States will be responsible for monitoring compliance with the requirements attached to the provision of such services.*”⁴⁹

108. Article 9(1) of the Proposal, specified under recital 22, sets out three different types of data sharing services:
- under letter (a), intermediary between data holders which are legal persons and potential data users;
 - under letter (b), intermediation services between data subjects and potential data users;
 - under letter (c), ‘data cooperatives’.
109. Having regard to the first type of data sharing service, Article 9(1)(a) refers to “*intermediation services between data holders which are legal persons and potential data users, including making available the technical or other means to enable such services; those services may include bilateral or multilateral exchanges of data or the creation of platforms or databases enabling the exchange or joint exploitation of data, as well as the establishment of a specific infrastructure for the interconnection of data holders and data users.*”

⁴⁹ Explanatory Memorandum, page 7.

110. Recital (22) specifies: “*Providers of data sharing services (data intermediaries) are expected to play a key role in the data economy, as a tool to facilitate the aggregation and exchange of substantial amounts of relevant data. Data intermediaries offering services that connect the different actors have the potential to contribute to the efficient pooling of data as well as to the facilitation of bilateral data sharing. Specialised data intermediaries that are independent from both data holders and data users can have a facilitating role in the emergence of new data-driven ecosystems independent from any player with a significant degree of market power. This Regulation should only cover providers of data sharing services that have as a main objective the establishment of a business, a legal and potentially also technical relation between data holders, including data subjects, on the one hand, and potential users on the other hand, and assist both parties in a transaction of data assets between the two. It should only cover services aiming at intermediating between an indefinite number of data holders and data users, excluding data sharing services that are meant to be used by a closed group of data holders and users.*”
111. In light of the above, the EDPB and the EDPS consider that the issue referred to under the general remarks of this Joint Opinion as overarching concern, namely the risk that the Proposal creates a parallel set of rules, which are not consistent with the GDPR, is particularly evident with reference to Chapter III of the Proposal. Indeed, it is unclear the interplay of the provisions under Article 9 of the Proposal, referring to ‘data holders’, ‘potential data users’, ‘the exchange or joint exploitation of data’, ‘the interconnection of data holders and data users’, with the rules and principles of the GDPR.
112. We recall that the data sharing service as platform “intermediating between an indefinite number of data holders and data users” excluding the use by a closed group of data users, in so far as the intermediation relates to personal data, shall be compliant in particular with the principle of data protection by design and by default under Article 25 of the GDPR⁵⁰.

⁵⁰ See Article 25(2): “The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.”

See also EDPB Guidelines 4/2019 on the principle of privacy by design and by default, at page 20:

“Key design and default purpose limitation elements may include:

- Predetermination – The legitimate purposes shall be determined before the design of the processing.
- Specificity – The purposes shall be specified and explicit as to why personal data is being processed.
- Purpose orientation – The purpose of processing should guide the design of the processing and set processing boundaries.
- Necessity – The purpose determines what personal data is necessary for the processing.
- Compatibility – Any new purpose must be compatible with the original purpose for which the data was collected and guide relevant changes in design.
- Limit further processing – The controller should not connect datasets or perform any further processing for new incompatible purposes.
- Limitations of reuse – The controller should use technical measures, including hashing and encryption, to limit the possibility of repurposing personal data. The controller should also have organisational measures, such as policies and contractual obligations, which limit reuse of personal data.

113. The EDPB and the EDPS also point out to the data protection principles of transparency (and purpose limitation) of the processing of personal data. As stated in the WP29 Guidelines on transparency “*the data subject should ... be able to determine in advance what the scope and consequences of the processing entails*” (...) “*namely the kind of effect will the specific processing described in a privacy statement/notice actually have on a data subject*”.⁵¹
114. The concept of data sharing service as platform “intermediating between an indefinite number of data holders and data users”, as kind of open data marketplace, would be contrary to the aforesaid data protection principles of privacy by design and by default, transparency and purpose limitation if the platform does not allow a pre-selection of and prior information about the purposes and users of her or his personal data by and to the data subject. For the sake of clarity, the Proposal should specify, at least in a recital, this aspect.
115. The scope of the notion of data intermediary between data holders and legal persons is also unclear, and hence should be better specified⁵².
116. As a general observation, it can also be remarked that the Proposal does not specify how (according to which GDPR legal basis) data sharing service providers will collect personal data for the sharing purposes.
117. It is also unclear whether data sharing service providers can intermediate data allowed for re-use by public sector bodies under Chapter II of the Proposal.
118. It is also key, for transparency reasons and to increase (rather than decrease) the level of citizens' trust, to make clear in the Proposal that the data sharing service will be provided upon payment of a

- Review – The controller should regularly review whether the processing is necessary for the purposes for which the data was collected and test the design against purpose limitation.”

⁵¹ Article 29 Working Party, Guidelines on transparency under Regulation 2016/679 WP260, rev.01, page 7.

⁵² Recital 22 specifies: “[...] Providers of **cloud services** should be excluded, as well as **service providers that obtain data from data holders, aggregate, enrich or transform the data and licence the use** of the resulting data to data users, without establishing a direct relationship between data holders and data users, for example **advertisement or data brokers, data consultancies, providers of data products resulting from value added** to the data by the service provider. At the same time, data sharing service providers should be allowed to make **adaptations to the data exchanged, to the extent that this improves the usability** of the data by the data user, where the data user desires this, such as to convert it into specific formats. In addition, **services that focus on the intermediation of content, in particular on copyright-protected content, should not be covered** by this Regulation.

Data exchange platforms that are exclusively used by one data holder in order to enable the use of data they hold as well as platforms developed in the context of objects and devices connected to the Internet-of-Things that have as their main objective to ensure functionalities of the connected object or device and allow value added services, should not be covered by this Regulation. ‘Consolidated tape providers’ in the sense of Article 4 (1) point 53 of Directive 2014/65/EU of the European Parliament and of the Council as well as ‘account information service providers’ in the sense of Article 4 point 19 of Directive (EU) 2015/2366 of the European Parliament and of the Council should not be considered as data sharing service providers for the purposes of this Regulation. Entities which restrict their activities to facilitating use of data made available on the basis of data altruism and that operate on a not-for-profit basis should not be covered by Chapter III of this Regulation, as this activity serves objectives of general interest by increasing the volume of data available for such purposes.”

'price' by data holders and data users. This aspect can be deducted from the wording of Article 11(3) of the Proposal⁵³, but is unclear and incomplete (it does not provide a clear picture of the monetary transactions accompanying the processing of personal data). The clear incentive to 'monetize' personal data also increases the importance of checks on data protection compliance⁵⁴. Regrettably, in this regard, as well as in relation to the other chapters of the Proposal, the impact assessment⁵⁵ does not take the data protection risks into account.

119. Moreover, the EDPB and the EDPS observe that the Proposal does not provide a clear picture, for instance via examples in the recitals, of the 'use cases' of data sharing services (whose 'monetary transaction aspect', as highlighted, shall be made clear to the public and to the persons concerned when this is the case). For instance, recital (22) specifies what is not a data exchange platform to be considered 'data intermediary': "*Data exchange platforms that are exclusively used by one data holder in order to enable the use of data they hold as well as platforms developed in the context of objects and devices connected to the Internet-of-Things that have as their main objective to ensure functionalities of the connected object or device and allow value added services, should not be covered by this Regulation*", but does not provide in this regard the envisaged use case.

3.4.1 Data intermediaries under Article 9(1) (b): intermediation services between data subjects and potential data users⁵⁶.

120. The EDPB and the EDPS note that the provisions related to intermediation services between data subjects that seek to make their personal data available and potential data users in the exercise of the rights provided in Regulation (EU) 2016/679, as per article 9(1)(b), is to be applied without prejudice to the effective application of the data subjects' rights and data controller's obligations as per the GDPR.
121. The Proposal however does not specify the modalities upon which such service providers would effectively assist individuals in exercising their rights under the GDPR nor provides indication as to which personal data processing such assistance would apply and towards which data users precisely⁵⁷.
122. The EDPB and the EDPS first of all consider that the effective exercise of data subjects' rights and the possible modalities for such exercise are provided for by the GDPR, under the monitoring of national supervisory authorities as per Article 51 of that same Regulation. The lack of clarity on the precise

⁵³ Article 11(3) of the Proposal lays down: "the provider shall ensure that the procedure for access to its service is fair, transparent and non-discriminatory for both data holders and data users, including as regards **prices**."

⁵⁴ In this regard, the EDPB is developing guidance on the collection and use of personal data against financial remuneration.

⁵⁵ Impact Assessment accompanying the Data Governance Act, SWD(2020) 295 final, available at:
<https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2020:0295:FIN:EN:PDF>

⁵⁶ Article 9(1)(b) of the Proposal refers to: "intermediation services between data subjects that seek to make their personal data available and potential data users, including making available the technical or other means to enable such services, in the exercise of the rights provided in Regulation (EU) 2016/679."

⁵⁷ Article 11(10) of the Proposal is still quite vague in its wording "the provider offering services to data subjects **shall act in the data subjects' best interest when facilitating the exercise of their rights**, in particular by advising data subjects on potential data uses and standard terms and conditions attached to such uses;"

modalities in the assistance provided for the exercise of data subjects' rights, as well as on the recipients of such process and their obligations towards data subjects may lead to further legal uncertainties in effectively exercising data subjects' rights as per the GDPR.

123. **The EDPB and the EDPS would therefore recommend that the Proposal reflects the EU legal framework (GDPR) according to which such modalities, as well as related obligations applicable to data sharing services providers and recipients, can be further specified by the European Data Protection Board, in accordance with Article 70 of the GDPR⁵⁸.**
124. It is also unclear whether the intermediation services under letter (b) of Article 9(1) of the Proposal, for which a definition is not provided under its Article 2, refer to and refer only to (and to which extent) Personal Information Management Systems (PIMS). The EDPB and the EDPS point out to the difference between PIMS, allowing management of personal data and facilitating the exercise of data subjects' rights ('interfacing with the data subject')⁵⁹, on the one hand, and business to business data sharing service providers (whose correlation with 'data brokers' is unclear), on the other hand. It is in relation to the latter, where the data subject is more far-way and at risk of not having a clear overview and control over the sharing of his or her personal data, that criticalities under the data protection viewpoint may be higher⁶⁰.
125. However, in all cases transparency, fairness and purpose limitation principles shall apply.
126. In its Opinion on PIMS, the EDPS pointed out that "*In any event, it is crucial to ensure the transparency of the business model vis-à-vis the individuals whose data are being processed so that they are aware of the interests at stake (of PIMS and other service providers) and can use PIMS in full awareness*"⁶¹.

⁵⁸ In this regard, the EDPB is currently working on guidelines on data subject rights.

⁵⁹ See the EDPS Opinion on Personal Information Management Systems, 20 October 2016, available at: https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf

⁶⁰ See EDPS Opinion on the European Strategy for Data, paragraph 20: "At the same time, the EDPS underlines the need of caution with regard to the role of data brokers that are actively engaged in the collection of huge datasets, including personal data from different sources. They tap into a variety of data sources used for data-related services, such as data that are disclosed for other unrelated purposes; data from public registers (open data), as well as data "crawled" from the Internet and social media, often in violation of data protection legislation. In this context, the EDPS notes that the activities of big data brokers are under increased scrutiny and are investigated by a number of national data protection authorities."

⁶¹ See page 13, para. 52, of the EDPS Opinion on Personal Information Management Systems, 20 October 2016, available at: https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf

See also para 53, page 13: "*The model of PIMS seems to invite a debate over who 'owns' our personal data. Individuals in the EU have a fundamental right to the protection of their personal data, based upon Article 8 of the EU Charter of Fundamental Rights. Detailed rights and obligations relating to the exercise of this right are regulated in further detail in the recently adopted GDPR. These issues are not specific to PIMS: personal data is often perceived as the 'currency' we pay for so-called 'free' services on the internet. This trend does not, however, mean that personal data of individuals can legally be considered as property which can be traded freely as any other property on the market. On the contrary, as a matter of principle PIMS will not be in a position to 'sell' personal data, but rather, their role will be to allow third parties to use personal data, for specific purposes, and specific periods of time, subject to terms and conditions identified by the individuals themselves, and all other safeguards provided by applicable data protection law.*"

127. The Proposal provides some clarifications related to providers of data sharing services not established in the Union in order to determine whether such a provider is offering services within the Union. This specification, under recital 27 of the Proposal, seems in line with recital (23) of the GDPR. It might be useful, for the sake of legal certainty, specifying that, in case of processing of personal data, the aforesaid data sharing service providers not established in the Union are subject to the rules and principles of the GDPR.

3.4.2 Data intermediaries under Article 9(1) (c): 'data cooperatives'

128. The EDPB and the EDPS underline that the notion of "service of data cooperatives", introduced in Article 9(1)(c) of the Proposal⁶², remains unclear both in terms of nature and obligations. In this regard, a clear definition of such data sharing services providers, as well as their applicable obligations, should be introduced in order to avoid any legal uncertainty in the provision of such services.
129. While the Proposal specifies that data cooperatives "*seek to strengthen the position of individuals in making informed choices before consenting to data use, influencing the terms and conditions of data user organisations attached to data use or potentially solving disputes between members of a group on how data can be used when such data pertain to several data subjects within that group*"⁶³, it is to be recalled that transparency obligations, as well as the conditions for the valid consent of the data subject as per Article 6(1)(a) of Regulation (EU) 2016/679 and the condition for the processing of personal data under this legal basis, are defined and provided for by that same regulation.
130. **The EDPB and the EDPS therefore consider that the position of individuals in making informed choice, or the solving of potential dispute on how data can be used, are not to be considered as negotiable conditions but rather as data controllers' obligations as per Regulation (EU) 2016/679.** In this regard, it is also to be pointed out that the reference in Recital (24) of the Proposal to data that would "pertain" to several data subject, insofar as it relates to personal data, may not be consistent with the definition of personal data as per Regulation (EU) 2016/679⁶⁴, which refers to "any information relating to an identified or identifiable natural person".
131. Furthermore, as recalled in Recital (24) of the Proposal, "*the rights under Regulation (EU) 2016/679 can only be exercised by each individual and cannot be conferred or delegated to a data cooperative*". The EDPB and the EDPS consider that the articulation of such principles with the possibility for data cooperatives to be conferred powers to "negotiate terms and conditions for data processing before they consent" is unclear at least, if not directly contradictory. Indeed, the "terms and conditions" for the processing of personal data are - as a matter of fact - those enshrined in the GDPR and, therefore, they cannot be amended or superseded by means of a contract or other type of private arrangements.

⁶² Article 9(1)(c) of the Proposal refers to "services of data cooperatives, that is to say services supporting data subjects or one-person companies or micro, small and medium-sized enterprises, who are members of the cooperative or **who confer the power to the cooperative to negotiate terms and conditions for data processing before they consent, in making informed choices before consenting to data processing, and allowing for mechanisms to exchange views on data processing purposes and conditions that would best represent the interests of data subjects or legal persons.**"

⁶³ Recital (24) of the Proposal.

⁶⁴ Definition under Article 4(1) of the GDPR.

3.4.3 Article 10: notification regime - general requirements to be eligible for registration - content of the notification; outcome (and timing) of the notification. Article 11: conditions for providing data sharing services

132. Chapter III of the Proposal establishes an obligation for providers of data sharing services as described under Article 9(1) to submit a notification to the competent authority (mandatory notification). Article 10(1) and (2) provide rules on the identification of the jurisdiction of the Member State for the purposes of the Proposal. This is the jurisdiction of the Member State of the main establishment of the data sharing service provider or the Member State of establishment of the legal representative of the data sharing service provider not established in the Union.
133. The information to be included in the notification is provided under Article 10(6), letters (a)-(h) of the Proposal⁶⁵. In addition, Article 10(7) lays down that "*At the request of the provider, the competent authority shall, within one week, issue a standardised declaration, confirming that the provider has submitted the notification referred to in paragraph 4.*"
134. The notification regime, as highlighted in the Explanatory Memorandum, "consists of a *notification obligation with ex post monitoring of compliance with the requirements to exercise the activities by the competent authorities of the Member States*"⁶⁶. This aspect is further specified under recitals (30) and (31) of the Proposal⁶⁷.
135. Hence, the 'vetting' of the data sharing service provider is limited to the verification by the competent authority of the (mainly formal) requirements set out in Article 10 and shall occur within a very short time-limit (one week from the date of notification).

⁶⁵ "The notification shall include the following information:

(a) the name of the provider of data sharing services;
(b) the provider's legal status, form and registration number, where the provider is registered in trade or in another similar public register;
(c) the address of the provider's main establishment in the Union, if any, and, where applicable, any secondary branch in another Member State or that of the legal representative designated pursuant to paragraph 3;
(d) a website where information on the provider and the activities can be found, where applicable;
(e) the provider's contact persons and contact details;
(f) a description of the service the provider intends to provide;
(g) the estimated date for starting the activity;
(h) the Member States where the provider intends to provide services."

⁶⁶ Explanatory Memorandum, page 5.

⁶⁷ "(30) A notification procedure for data sharing services should be established in order to ensure a data governance within the Union based on trustworthy exchange of data. The benefits of a trustworthy environment would be best achieved by imposing a number of requirements for the provision of data sharing services, but **without requiring any explicit decision or administrative act by the competent authority for the provision of such services**.

(31) In order to support effective cross-border provision of services, the data sharing provider should be requested to **send a notification only to the designated competent authority from the Member State where its main establishment is located or where its legal representative is located**. Such a **notification should not entail more than a mere declaration of the intention to provide such services and should be completed only by the information set out in this Regulation**." (emphasis added)

136. In this regard, the EDPB and the EDPS note that the ‘vetting’ regime is almost ‘declarative’ and that the Commission has opted for the most ‘loose’ regime (as opposed for instance to an authorization regime). The EDPB and the EDPS observe that, at least with regard to the processing of personal data, the regime should be more protective (that is, provide more checks and safeguards for the data subjects, including on the crucially important data protection aspects). This would also allow ensuring the higher level of trust aimed at by the Commission.
137. In order to address this concern, in particular Recital 31 of the Proposal should be amended.
138. According to the data protection principle of accountability, data sharing service providers shall be able among others to demonstrate that they put in place policies and procedures that allow data subjects to easily exercise their individual data protection rights (procedures for ensuring compliance with data subjects’ rights), and should document the decisions about the data sharing (including in particular the purposes for which the personal data will be shared and the recipients or categories of recipients to whom they will be disclosed), evidencing their compliance with data protection law⁶⁸. These aspects (which should form the ‘core’ of the labelling envisaged by the Proposal⁶⁹) will have the effect of creating greater trust in data sharing service providers by the public.
139. The EDPB and the EDPS also remark that the provisions of data sharing services, as laid down under Article 11, shall be subject to conditions under (1)-(11). In this regard, the EDPB and the EDPS notice that while reference is made among the conditions to compliance with competition rules (under (9)), these (exhaustively listed) conditions do not include compliance with data protection rules.
140. In light of the elements above, and considering the possible risk for data subject in the personal data processing that may be undertaken by data sharing service providers, the EDPB and the EDPS consider that the declaratory notification regime as laid down in the Proposal does not provide for a sufficiently stringent vetting procedure applicable to such services. The EDPB and the EDPS recommend exploring alternative procedures which should notably take into account a more systematic inclusion of accountability and compliance tools for the processing of personal data as per the GDPR, in particular the adherence to a code of conduct or certification mechanism.

⁶⁸ According to Article 30 of the GDPR: “Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information: (a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer; (b) the purposes of the processing; (c) a description of the categories of data subjects and of the categories of personal data; (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; (f) where possible, the envisaged time limits for erasure of the different categories of data; (g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1). [...]”

⁶⁹ The Impact Assessment of the Proposal refers to labelling or certification, among others, at page 19 “Mutual recognition of certification/labelling mechanisms and of a trust scheme for data altruism will make it possible to collect and use the data at the necessary scale.”; page 25 “certification/labelling framework for data intermediaries”; page 26: “A certification or labelling framework would allow novel data intermediaries to increase their visibility as trustworthy organisers/orchestrators of data sharing or pooling.”

141. It can also be observed that the safeguards provided in Chapter IV of the Proposal for data altruism organizations (Article 18, transparency requirements; Article 19, specific requirements) are not foreseen by the Proposal having regard to data sharing service providers, despite the possible impact also of these data sharing services on the rights and freedoms of the persons concerned.
142. This difference between the two notification regimes might give raise to interpretation *a contrario* that the requirements established for data altruism organizations and relating to the protection of personal data insofar as personal data are processed (for instance, informing data holders about any processing outside the Union⁷⁰) do not apply to data sharing service providers.
143. In this regard, the EDPB and the EDPS notice in particular that organisations involved in ‘data pooling’ or data sharing arrangements should adhere to certain common standards, whose supervision by independent data protection authorities shall be expressly recalled by the Proposal, related not only to the conditions for interoperability, but also to the conditions for ensuring the lawfulness of the processing of personal data and facilitating the exercise of data subject rights (e.g., through joint controllers’ arrangements pursuant to Article 26 of the GDPR).
144. Moreover, the EDPB and the EDPS notice that the Proposal refers to scenarios (use of metadata for the development of the data sharing service, under Article 11(2); continued access by data holders and data users after insolvency of the data sharing provider to data stored by the latter, under Article 11(6)) which need specifications in order to bring them in line with rules and principles on the protection of personal data.
145. The EDPB and the EDPS also remark that the comments made under the general remarks of this opinion, related to the definitions used in the Proposal and to the issue of the legal basis under the GDPR for the processing of personal data, are also relevant having regard to the provisions of Chapter III of the Proposal.
146. Furthermore, with particular reference to the aim of ensuring better control on the access and use of personal data by the data subject, we recall that the principle of purpose limitation is of special importance having regard to business-to-business data intermediaries. Recital (26) of the Proposal⁷¹, which seems to identify the purpose of the processing of personal data with the intermediation in the sharing of data, without further specifications, might raise concerns from a data protection viewpoint⁷².

⁷⁰ Article 19(1)(b) of the Proposal.

⁷¹ Recital (26) of the Proposal: “A key element to bring trust and more control for data holder and data users in data sharing services is the neutrality of data sharing service providers as regards the data exchanged between data holders and data users. It is therefore necessary that data sharing service providers **act only as intermediaries** in the transactions, and do not use the data exchanged for **any other purpose**. [...]”

⁷² See also Article 2(4) of the Proposal: ‘metadata’ means data collected on any activity of a natural or legal person **for the purposes of the provision of a data sharing servicethe purpose of joint or individual use of the shared dataother purposes than to put them at the disposal of data users.**”

147. The EDPB and the EDPS consider that the remarks made under Section 3.3 of this Joint Opinion concerning the reuse of personal data held by public sector bodies are also relevant having regard to data sharing services:

- any sharing or access to personal data must be strictly defined in scope and purpose and must occur in full compliance with the GDPR, taking into account the requirements of lawfulness, purpose limitation and the legitimate expectations of the data subjects;
- it should be clear that each ‘actor’ of the data processing chain, including the data sharing service provider and the user(s), shall provide the data subjects with the information under Article 13 and 14 of the GDPR (oftentimes, Article 14, applicable where personal data have not been obtained by the data subject, will be the relevant provision of the GDPR in this context). We recommend adding in this regard that the data sharing service provider shall provide the data subject with user-friendly tools showing him/her a comprehensive view of how his/her personal data are shared, as well as a user-friendly tool to withdraw consent in case the service provided consists of a tool for obtaining consent from data subjects with regard to the processing of their personal data under Article 11(11) of the Proposal
- the data protection impact assessment (DPIA) is a key tool to ensure that data protection requirements are properly taken into account and the rights and interests of individuals are adequately protected, so as to foster their trust in the re-use mechanism. Therefore, the EDPB and EDPS recommends to include in the text of the Proposal that **a DPIA must be performed by data sharing service providers (and by the data user) in case of data processing falling under Article 35 of the GDPR**. Indeed, the data sharing envisaged under the Proposal may involve large-scale processing, which combines data from a variety of sources, potentially involving special categories of data and/or personal data of vulnerable groups of data subjects. In this case, data controllers have the obligation to perform a DPIA in accordance with Article 35 of the GDPR. Moreover, whenever possible, the results of such assessments, as a trust and transparency-enhancing measure, shall be made public by the data sharing service provider as well as by the user(s).

3.4.4 Articles 12 and 13: competent authorities and monitoring of compliance (with Articles 10 and 11).

148. Article 12(3) of the Proposal provides that “*The designated competent authorities, the data protection authorities, the national competition authorities, the authorities in charge of cybersecurity, and other relevant sectorial authorities shall exchange the information which is necessary for the exercise of their tasks in relation to data sharing providers.*”
149. This wording provides for an even minor role for data protection authorities than the wording used by the Proposal in relation to data altruism organisations⁷³, which refers to “cooperation with data protection authorities”.

⁷³ Article 20(3): “The competent authority shall undertake its tasks [of authority responsible for the register of recognised **data altruism organizations** and for the monitoring of compliance with the requirements of Chapter

150. In this regard, as highlighted in Section 3.7 of this Joint Opinion, the EDPB and the EDPS recall that many provisions of this Chapter as well as of the other Chapters of the Proposal relate to the processing of personal data and that the data protection authorities are the authorities ‘constitutionally’ competent for the supervision related to the protection of personal data pursuant to Article 8 of the Charter and Article 16 TFEU.
151. Having regard to Article 13 of the Proposal, monitoring of compliance, notwithstanding recital (28) which states that the Proposal should be without prejudice to the responsibility of supervisory authorities to ensure compliance with the GDPR, the EDPB and the EDPS consider that the governance and monitoring of compliance should be better defined in order to ensure a more appropriate vetting of data sharing service providers (and data altruism organisations) including on compliance with the GDPR; and to avoid, at the same time, any overlap or conflict of attribution between the authorities established under the Proposal (which, according to the wording of Articles 12(3) -and 20(3)-, are not data protection authorities) and the data protection authorities.
152. **The EDPB and EDPS therefore consider that such better definition of governance would be provided by the designation of data protection authorities as the main competent authorities to monitor and supervise compliance with the provisions of Chapter III of the Proposal.**
153. The designation of data protection authorities as the main competent authorities for the supervision and enforcement of the provisions under Chapter III of the Proposal would also ensure a more consistent regulatory approach across Member State and therefore contribute to the consistent application of the Proposal. As per their competence and tasks under the GDPR, data protection authorities have already specific expertise in the monitoring of the compliance of data processing, the auditing of specific data processing activities and data sharing, the assessment of the adequate measures to ensure a high level of security for the storage and transmission of personal data, as well as in promoting awareness among controllers and processors of their obligation related to the processing of personal data.
154. The designation of data protection authorities as main competent authority for the supervision and enforcement of the provisions under Chapter III shall be supported with the foreseen provision under Article 12(3) allowing for the exchange of information between the data protection authorities, the national competition authorities, the authorities in charge of cybersecurity, and other relevant sectorial authorities in order to ensure a coherent application of these provisions.

IV of the Proposal] **in cooperation with the data protection authority**, where such tasks are related to processing of personal data, and with relevant sectoral bodies of the same Member State. For any **question requiring an assessment of compliance with Regulation (EU) 2016/679**, the competent authority shall first seek an opinion or decision by the competent supervisory authority established pursuant to that Regulation and comply with that opinion or decision.”

It also has to be noted that recital 28 -having regard to **providers of data sharing services**- specifies that “this Regulation should be **without prejudice to** the obligation of providers of data sharing services to comply with Regulation (EU) 2016/679 and **the responsibility of supervisory authorities to ensure compliance with that Regulation.**” The same specification is **not** made having regard to data altruism organizations.

- 155. In addition, the EDPB and EDPS consider that, when monitoring compliance, the power of the competent authorities cannot be limited to “the power to request information”, as it appears from Article 13(2) of the Proposal. This limitation definitely stems from the declaratory nature of the “labelling regime” envisaged by the Proposal, albeit it is not adequate to the level of vetting the labelling requires, due to the high expectations of data protection compliance resulting from such labelling, especially vis-à-vis data subjects.
- 156. Finally, the EDPB and EDPS emphasise that adequate resources should be provided to the data protection authorities in order to allow them to effectively and efficiently perform the necessary supervision.

3.5 Data altruism

3.5.1 Interplay between data altruism and consent under the GDPR

- 157. The concept of “data altruism” referred to in the Proposal covers situations where natural or legal persons make data voluntarily available for reuse, without compensation, for “purposes of general interest, such as scientific research purposes or improving public services”⁷⁴.
- 158. It can be argued that the Proposal does not “create” but “formalizes/codifies” the possibility for data holders (defined as including data subjects by the Proposal) to make data available voluntarily, already envisaged in the GDPR. Indeed, a data subject can already consent to the processing of personal data relating to her or him for, among others, scientific research purposes.
- 159. Despite the definition provided under Article 2(10) of the Proposal (“‘data altruism’ means the consent by data subjects to process personal data pertaining to them, or permissions of other data holders to allow the use of their non-personal data without seeking a reward, for purposes of general interest, such as scientific research purposes or improving public services”), the concept of “data altruism” is still not clearly and sufficiently defined. In particular, it is unclear whether the consent envisaged in the Proposal corresponds to the notion of “consent” under the GDPR, including the conditions for the lawfulness of such consent. In addition, it is unclear the added value of ‘data altruism’, taking into account the already existing legal framework for consent under the GDPR, which provides for specific conditions for the validity of consent.
- 160. The GDPR and the Proposal concurrently apply in case of processing of personal data by data altruism organisations. The EDPB and EDPS support the objective of facilitating the processing of personal data for well-defined purpose(s) of general interest, still such aim shall be achieved in full compliance with the applicable data protection rules and principles. In particular, the EDPB and the EDPS underline that one of the main objectives of the GDPR is to ensure that the data subject keeps control over her or his personal data. In this context, the EDPB and EDPS underline that **all requirements related to the consent, as set in the GDPR, need to be fulfilled**.
- 161. The EDPB and the EDPS reiterate that **the fundamental right to the protection of personal data cannot in any case be ‘waived’ by the individual concerned**, be it through an ‘act of altruism’ related

⁷⁴ Article 2(10) of the Proposal.

to personal data. The data controller (the data altruism organisation) remains fully bound by the personal data rules and principles even when the data subject has given consent to the data altruism organisation for the processing of personal data relating to him or her for one or more specified purpose(s).

162. In light of the above, the Proposal should specify in the substantive part that it refers to consent as defined under Article 4(11) of the GDPR and that, pursuant to Article 7(3), the data altruism organisation shall make as easy to withdraw consent as to provide it⁷⁵.
163. The EDPB and the EDPS also stress the fact that data processed by the data altruism organisations may include special categories of personal data, e.g. data concerning health.
164. The EDPB and the EDPS also underline that, in line with the principle of data minimisation, where it is possible and adequate to the purpose, data should be processed in anonymised form.
165. The EDPB and the EDPS welcome that the Proposal specifies under Article 22(3) that where personal data is provided to the data altruism organisation, the consent form shall ensure that individuals are able to provide and withdraw consent, for a specific data processing operation, in line with the GDPR.
166. In this regard, the EDPB and the EDPS consider that the rules for withdrawal of consent, including its consequences, should be clear. It should be clear in particular how both the data altruism organisation and the data users comply with the requests for withdrawal, including by deleting the personal data in accordance with Article 17(1)(b) GDPR. The EDPB and the EDPS recall that, when taking decisions on ‘data altruism’, data protection impact assessments may have to be performed by data altruism organizations in accordance with Article 35 of the GDPR.
167. Scientific research often involves the processing and sharing of special categories of personal data on a large scale and thus, in certain cases, the latter could be considered a high-risk data processing according to the GDPR. Furthermore, data protection impact assessments in this context should be conducted with the involvement of the data protection officer (DPO) and of an ethical review board and, where possible and as a matter of good practice, should be made public, or a summary thereof.
168. According to the GDPR, 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.
169. Recital 33 of the GDPR underlines that 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

⁷⁵ See EDPB Guidelines 5/2020 on consent, at paras 121-122:

“121. Article 6 sets the conditions for a lawful personal data processing and describes six lawful bases on which a controller can rely. The application of one of these six bases must be established prior to the processing activity and in relation to a specific purpose.

122. It is important to note here that if a controller chooses to rely on consent for any part of the processing, they must be prepared to respect that choice and stop that part of the processing if an individual withdraws consent. Sending out the message that data will be processed on the basis of consent, while actually some other lawful basis is relied on, would be fundamentally unfair to individuals.”

should be allowed to give their consent to certain areas of scientific research when in compliance with recognised ethical standards for scientific research⁷⁶. This is also reflected in recital (38) of the Proposal.

170. However, the EDPB and the EDPS underline that granting this kind of consent for purposes of general interest⁷⁷ as such (not strictly defined and referring to a possibly different and much broader scope than scientific research) is not allowed under the GDPR.
171. Indeed, the Proposal, in its recital 35 refers to “purposes of general interest” by providing (not a definition, but) a non-exhaustive list of examples, which includes applied and privately funded research and technological development and data analytics⁷⁸.
172. **In light of the above, the EDPB and the EDPS consider that the Commission should better define the purposes of general interest of such “data altruism”. The EDPB and EDPS consider that this lack of definition may lead to legal uncertainty, as well as to lower the level of protection of personal data in the EU. For instance, the requirement for the data altruism organization to inform the data holder (including the data subject) “about the purposes of general interest for which it permits the processing of their data by a data user” shall be in line with the principle according to which data shall be collected for specified, explicit and legitimate purposes and not further processed in a**

⁷⁶ See recently adopted EDPB Guidelines on consent, Guidelines 5/2020, in particular on consent for scientific research, at pages 30-32.

⁷⁷ See EDPB Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, at paras 42-45:

“42. As a general rule, data shall be “collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes” pursuant to Article 5 (1) (b) GDPR.

43. However the “compatibility presumption” provided by Article 5(1)(b) GDPR states that “further processing for [...] **scientific research purposes** [...] shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes”. This topic, due to its horizontal and complex nature, will be considered in more detail in the planned **EDPB guidelines on the processing of health data for the purpose of scientific research**.

44. Article 89 (1) GDPR stipulates that the processing of data for research purposes “shall be subject to **appropriate safeguards**” and that those “safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner”.

45. The requirements of Article 89(1) GDPR emphasise the importance of the data minimisation principle and the principle of integrity and confidentiality as well as the principle of data protection by design and by default (see below). Consequently, considering the sensitive nature of health data and the risks when re-using health data for the purpose of scientific research, strong measures must be taken in order to ensure an appropriate level of security as required by Article 32(1) GDPR.”

See also EDPB document in response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research, adopted on 2 February 2021.

⁷⁸ Recital 35: “Such purposes would include healthcare, combating climate change, improving mobility, facilitating the establishment of official statistics or improving the provision of public services. Support to scientific research, including for example technological development and demonstration, fundamental research, applied research and privately funded research, should be considered as well purposes of general interest. This Regulation aims at contributing to the emergence of pools of data made available on the basis of data altruism that have a sufficient size in order to enable data analytics and machine learning, including across borders in the Union.”

manner that is incompatible with those purposes (principle of purpose limitation, under Article 5(b) of the GDPR. Hence, an exhaustive list of clearly defined purposes should be provided in the Proposal. At the same time, the EPDB and the EDPS notice the specification made in recital 38 of the Proposal⁷⁹. These specification shall be included in the substantive part of the Proposal and not only in the recital and be accompanied by a clear distinction in the Proposal between:

- consent to areas of scientific research;
- further processing for scientific or historical or statistical purposes;
- and the processing for purposes of general interest (to be defined in the Proposal).

173. Moreover, the EDPB and the EDPS notice that the term “data repositories” in recital (36)⁸⁰, referred to only in this recital and not in the substantive part of the Proposal, and related to the processing of both personal and non-personal data, needs to be clarified.

[**3.5.2 Articles 16-17: registration regime - general requirements to be eligible for registration - content of the registration; outcome \(and timing\) of the registration;**](#)

174. Chapter IV of the Proposal establishes the possibility for organisations engaging in ‘data altruism’ to register as a “Data Altruism Organisation recognised in the Union”⁸¹ with the declared aim of increasing citizens’ trust in their operations. In this regard, the EDPB and EDPS underline that the Proposal does not clarify whether or not the registration is compulsory, nor whether the provisions under Chapter IV also apply in case that organisations engaging in data altruism are not registered.
175. The general requirements for registration are listed in Article 16; the requirements for registration are provided under Article 17, and notably at letters (a)-(i) of Article 17(4). The ‘vetting’ of the data altruism organization is limited to the verification by the competent authority of the requirements under Article 16 and 17(4) and shall occur within twelve weeks from the date of application. However, the kind of verification with which the competent authority is tasked is not defined by the Proposal.
176. In this respect, the EDPB and the EDPS remark that a regime providing stronger guarantees, in case of processing of personal data, would be more adequate to ensure appropriate checks and ultimately

⁷⁹ Recital (38): “Data Altruism Organisations recognised in the Union **should be able to collect relevant data directly from natural and legal persons or to process data collected by others.**

Typically, data altruism would rely on consent of data subjects in the sense of Article 6(1)(a) and 9(2)(a) and in compliance with requirements for lawful consent in accordance with Article 7 of Regulation (EU) 2016/679. In accordance with Regulation (EU) 2016/679, **scientific research purposes** can be supported by consent to **certain areas of scientific research** when in keeping with recognised ethical standards for scientific research or only to certain areas of research or parts of research projects.

Article 5(1)(b) of Regulation (EU) 2016/679 specifies that **further processing for scientific or historical research purposes or statistical purposes** should, in accordance with Article 89(1) of Regulation (EU) 2016/679, not be considered to be incompatible with the initial purposes.”

⁸⁰ Recital (36): “Legal entities that seek to support **purposes of general interest** by making available relevant data based on data altruism at scale and meet certain requirements, should be able to register as ‘Data Altruism Organisations recognised in the Union’. This could lead to the establishment of **data repositories**[...]

⁸¹ Recital (36) of the Proposal.

enhance trust, than the ‘lighter’ registration regime (almost a simply ‘declaratory’ regime) set out in the Proposal and similar to the one envisaged for data sharing service providers.

177. The EDPB and the EDPS underline that the fact that there is almost no requirement from a legal, technical and organizational point of view to become a “Data Altruism Organisation recognised in the Union” (or a “data sharing provider”) is problematic. For instance, an organisation, entitled pursuant to Article 15(3) of the Proposal to “refer to itself as a ‘Data Altruism Organisation recognised in the Union’ in its written and spoken communication” ('labelling effect'), will most probably collect personal data leveraging citizens' expectations in particular on full data protection compliance by the same organisation.
178. The EDPB and the EDPS stress that data altruism organisations need to be trusted entities. As regards the general requirements for registration (provided under Article 16 of the Proposal), the EDPB and EDPS also consider that the independence from the for-profit entities of the data altruism organization (e.g. legal, organizational, economical) is envisaged under Article 16(b) the Proposal should to be clarified⁸².
179. **In particular, the EDPB and the EDPS recommend introducing a direct reference to data protection requirements in Article 16, especially to the technical and organizational requirements enabling the application of data protection standards and the exercise of data subjects' rights.**
180. **In light of the elements above, and considering the possible impacts for data subjects with regard to the personal data processing that may be undertaken by data altruism organisation, the EDPB and the EDPS consider that the registration regime as laid down in the Proposal does not provide for a sufficiently stringent vetting procedure applicable to such organisation. The EDPB and the EDPS recommend exploring alternative procedures which should notably take into account a more systematic inclusion of accountability and compliance tools for the processing of personal data as per the GDPR, in particular the adherence to a code of conduct or certification mechanism.**

3.5.3 Articles 18-19: transparency requirements and “specific requirements to safeguard rights and interests of data subjects and legal entities as regards their data”

181. The EDPB and the EDPS notice that the requirements accompanying the registration regime should enhance but **not replace the obligations of the data altruism organizations as controllers or processors under the GDPR.**
182. The EDPB and the EDPS notice that recital 36 of the Proposal is unclear in this regard, since it seems to imply that means to withdraw consent shall be provided by the data altruism organization acting as processor⁸³. However, the qualification of data altruism organization as processor, instead of

⁸² “In order to qualify for registration, the data altruism organisation shall: [...] (b) operate on a not-for-profit basis and **be independent from any entity that operates on a for-profit basis;**” (emphasis added)

⁸³ Recital 36 laws down (bold added): “**Further safeguards** should include making it possible to **process relevant data within a secure processing environment** operated by the registered entity, **oversight mechanisms** such as ethics councils or boards to ensure that the data controller maintains high standards of scientific ethics, **effective**

controller, needs further assessment, since it does not seem to be the only possible scenario in the context of the Proposal.

183. The enabling effect of the registration (as data altruism organisation) should also be clearly defined, especially having regard to the aspect of the legal basis for the processing of personal data under the GDPR⁸⁴. In this regard, the EDPB and the EDPS reiterate that **the registration regime cannot replace the necessity of an appropriate legal ground for the processing of personal data under Article 6(1) of the GDPR** for the lawfulness of the data processing. In other words, according to the GDPR the processing of personal data shall be lawful only if and to the extent that at least one of the legal basis under Article 6(1) of the GDPR applies
184. Having regard to Article 18 of the Proposal, the EDPB and the EDPS have doubts as to how the independence of the data altruism organisation is preserved in cases where its funding is based on "*the fees paid by natural or legal persons processing the data*"⁸⁵ (i.e., data provided to these natural or legal persons by the data altruism organization). In addition, the EDPB and the EDPS consider that the Proposal should better explain in what situations the data altruism organisation can charge fees to natural or legal persons for the processing of the data 'conferred' by data subjects for 'data altruism'.
185. Also in this case, as remarked regarding the re-use of data held by public sector bodies, there is an issue related to incentives for the controller to encourage more processing of personal data, in this case more 'data altruism'. The qualification of data altruism organisations as registered entities having a not-for-profit character (recital 36) -which the EDPB and the EDPS welcome- only partially mitigates the aforesaid issue.
186. Moreover, the wording of recital 36 referring to requirements for data altruism organisations raises concerns since it refers to "voluntary compliance" also with regard to issues related to (mandatory) GDPR compliance⁸⁶.

technical means to withdraw or modify consent at any moment, **based on the information obligations of data processors under Regulation (EU) 2016/679** as well as **means for data subjects to stay informed** about the use of data they made available." (emphasis added)

⁸⁴ In this regard, recital 38 of the Proposal lays down as follows (bold added): "Data Altruism Organisations recognised in the Union **should be able to collect relevant data directly from natural and legal persons** or to process data collected by others. **Typically**, data altruism would rely on consent of data subjects in the sense of Article 6(1)(a) and 9(2)(a) and in compliance with requirements for lawful consent in accordance with Article 7 of Regulation (EU) 2016/679. In accordance with Regulation (EU) 2016/679, scientific research purposes can be supported by consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research or only to certain areas of research or parts of research projects. Article 5(1)(b) of Regulation (EU) 2016/679 specifies that further processing for scientific or historical research purposes or statistical purposes should, in accordance with Article 89(1) of Regulation (EU) 2016/679, not be considered to be incompatible with the initial purposes."

⁸⁵ See Article 18(1)(d) of the Proposal.

⁸⁶ Recital 36 (bold added): "[...] The **voluntary compliance** of such registered entities with a **set of requirements** should bring trust that the data made available on altruistic purposes is serving a general interest purpose. Such **trust** should result in particular from a **place of establishment within the Union**, as well as from the requirement that registered entities have a **not-for-profit character**, from **transparency** requirements and from **specific safeguards** in place to protect rights and interests **of data subjects and companies**. **Further safeguards** should

187. The recital is also inconsistent (unless prominence is given to the optional nature of the requirements under recital 36) with the substantive part of the Proposal, Article 17(3), which refers to data altruism organisations not established in the Union.
188. As regards Article 19 of the Proposal, the EDPB and EDPS are of the opinion that an explicit reference to Articles 13 and 14 of the GDPR should be added, in order to ensure consistency between this Article of the Proposal and the obligations concerning the transparency principle under the GDPR, and that the necessary information is provided by the data altruism organisation and by the data users to the data subject with regard to the processing of personal data relating to her or him.
189. Moreover, the EDPB and the EDPS consider that the current wording of Article 19(1)(a)⁸⁷ seems unclear and difficult to reconcile with the provisions of the GDPR .
190. As regards this Chapter of the Proposal, an explicit emphasis on providing anonymized data when it is possible and adequate for the purpose of data processing, in line with the principle of data minimisation, would also be of special importance to protect persons concerned from undue risks to their fundamental rights and freedoms, especially in case of processing of special categories of data.

[3.5.4 Articles 20 and 21: competent authorities for registration and monitoring of compliance](#)

191. With regard to article 20(3) of the Proposal, the EDPB and the EDPS consider that the governance and monitoring of compliance should be reinforced in order to ensure a more appropriate vetting of data altruism organizations including compliance with the GDPR, and to ensure that supervision on the provisions of the Proposal is clearly defined in a way that provides that, when it is a matter of personal data, data protection requirements are fully complied with and remain under the competence of the data protection authorities established under the GDPR.
192. The designation of data protection authorities as the main competent authorities for the supervision and enforcement of the provisions under Chapter IV of the Proposal would also ensure a more consistent regulatory approach across Member State and therefore contribute to the consistent application of the Proposal. As per their competence and tasks under the GDPR, data protection authorities have already specific expertise in the monitoring of the compliance of data processing, the auditing of specific data processing activities and data sharing, the assessment of the adequate measures to ensure a high level of security for the storage and transmission of personal data, as well as in promoting awareness among controllers and processors of their obligation related to the processing of personal data.

include making it possible to process relevant data within a **secure processing environment** operated by the registered entity, **oversight mechanisms** such as ethics councils or boards to ensure that the data controller maintains high standards of scientific ethics, effective **technical means to withdraw or modify consent** at any moment, based on the information obligations of data processors under Regulation (EU) 2016/679 as well as means for data subjects to **stay informed** about the use of data they made available.”

⁸⁷ Article 19(1)(a) states (bold added): “Any entity entered in the register of recognised data altruism organisations shall inform data holders: (a) **about the purposes of general interest for which it permits the processing of their data by a data user** in an easy-to-understand manner.”

193. In addition, the EDPB and EDPS consider that, when monitoring compliance, the power of the competent authorities cannot be limited to “the power to request information”, as it appears from Article 21(2) of the Proposal. This limitation definitely stems from the declaratory nature of the ‘labelling regime’ envisaged by the Proposal, albeit it is not adequate to the level of vetting the labelling requires, due to the high expectations of data protection compliance resulting from such labelling, especially vis-à-vis data subjects.
194. The EDPB and EDPS emphasise that adequate resources should be provided to the data protection authorities in order to allow them to effectively and efficiently perform the necessary supervision. Furthermore, the EDPB and the EDPS notice in this regard that recital (28) -which refers to providers of data sharing services- states that *“this Regulation should be without prejudice to the obligation of providers of data sharing services to comply with Regulation (EU) 2016/679 and the responsibility of supervisory authorities to ensure compliance with that Regulation.”* The same specification should also be made having regard to data altruism organizations.

[3.5.5 Article 22: European data altruism consent form](#)

195. Article 22 of the Proposal empowers the Commission to adopt, by means of implementing acts, a “European data altruism consent form”⁸⁸. In this regard, Article 22, as specified under recital 41, provides that the consent form shall be established via an implementing act by the Commission, assisted by the European Data Innovation Board, in consultation with the EDPB.
196. **In this regard, the EDPB and the EDPS consider that a more binding, better structured and institutionalized mechanism than a mere consultation of the EDPB should be established by the Proposal.**

[3.6 International transfers of data: Article 5\(9\)-\(13\); recital 17, 19; Article 30](#)

197. Even if the provisions of the Proposal relating to data transfers to third countries seem *a priori* limited to only non-personal data, issues of legal and policy consistency with the EU data protection legal framework are likely to emerge during their application, in particular when personal data and non-personal data of a dataset are inextricably linked.
198. However, although the exclusion of personal data seems to be the intention of the Commission, the limitation of the scope of transfers provisions to non-personal data is not always clearly reflected by the Proposal. In particular, Article 5(9) and 5(10), related to transfers of data held by public sector bodies, could apply to personal data if those personal data are at the same time confidential data or data protected by intellectual property rights⁸⁹.

⁸⁸ Article 22(1): “In order to facilitate the collection of data based on data altruism, the Commission may adopt implementing acts developing a European data altruism consent form. The form shall allow the collection of consent across Member States in a uniform format. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 29 (2).”

⁸⁹ See Article 5(10) of the Proposal: “Public sector bodies shall only transmit confidential data or data protected by intellectual property rights to a re-user which intends to transfer the data to a third country other than a country designated in accordance with paragraph 9 if the re-user undertakes: (a) to comply with the obligations imposed in accordance with paragraphs 7 to 8 even after the data is transferred to the third country; and (b) to

199. At the same time, the Proposal includes a provision (Article 5(11)) which could somehow be considered as more "protective" for non-personal data than for personal data, since according to the Proposal the Commission could ultimately adopt, by means of a delegated act⁹⁰, specific conditions for the transfer of non-personal data to certain third countries going as far as prohibition⁹¹.
200. The possibility for the Commission to adopt, by means of an implementing act⁹², 'adequacy decisions' for the transfer of non-personal data to a given third country is also likely to raise questions of interaction and consistency with the transfer tools provided for by the GDPR for the transfer of personal data to the same third country.
201. In any case, to ensure consistency with the data protection legal framework, it is important to recall in this regard that in case of 'mixed datasets' the GDPR applies, and in particular its Chapter V.
202. The EDPB and the EDPS notice that Article 30 of the Proposal⁹³ refers only to non-personal data and its paragraph 2 seems to mirror the provisions of Article 48 of the GDPR (with the difference that Article 30(2) introduces a limitation in time as to the international agreements concerned).
203. According to Article 30(3) of the Proposal, entities (the public sector body, the entity to which re-use was granted, the data sharing service provider, the data altruism organisation) receiving a decision to transfer or give access to non-personal data held in the Union by a court or an administrative authority of a third country shall seek the opinion of competent authorities or bodies pursuant to the Proposal in order to determine whether the applicable transfer conditions are met (Article 30(3), last sentence).
204. The consultation of the competent authority is necessary when the decision of the court or of the administrative authority of the third country "would risk putting the addressee in conflict with Union law or with the law of the relevant Member State" (Article 30(3)).⁹⁴
205. This provision, compared with Article 48 GDPR, seems to go one step further by requiring the consultation of the competent authority in specific cases. Therefore, in this regard, it could somehow

accept the jurisdiction of the courts of the Member State of the public sector body as regards any dispute related to the compliance with the obligation in point a)."'

⁹⁰ See recital (19) of the Proposal.

⁹¹ See recital (19) of the Proposal.

⁹² See Article 5(9)-(11) of the Proposal.

⁹³ Article 30, International access, included under Chapter VIII, final provisions.

⁹⁴ The aforesaid conditions in Article 30(3) seem sufficient to supersede the conditions in paragraph (2), and thus supersede the international rules referred to under this paragraph. Article 30(4) states that: "If the conditions in paragraph 2, or 3 are met, the public sector body, the natural or legal person to which the right to re-use data was granted under Chapter 2, the data sharing provider or the entity entered in the register of recognised data altruism organisations, as the case may be, shall, provide the minimum amount of data permissible in response to a request, based on a reasonable interpretation of the request." (bold added).

These provisions of the Proposal might be inconsistent with other Union or member State law, notably on judicial cooperation on criminal or civil matters. The relevance of this observation under data protection law is given by the fact that in case of misinterpretation of the notion of non-personal data, there is a high risk of public sector bodies, data sharing service providers, data altruism organizations, data re-users and data users, transferring personal data to a third country with (significantly) lower standard of protection for the persons concerned.

be considered as more "protective" for non-personal data than for personal data, since such notification is not envisaged under the GDPR.

3.7 Horizontal provisions on institutional settings; complaints; European Data Innovation Board (EDIB) expert group; delegated acts; penalties, evaluation and review, amendments to the single digital gateway regulation, transitional measures and entry into force

3.7.1 Article 23: requirements relating to competent authorities

206. Chapter V of the Proposal sets out the requirements for the functioning of the competent authorities designated to monitor and implement the notification framework for data-sharing service providers and entities engaged in data altruism. It stems from Chapters III and IV of the Proposal that such competent authorities are different from the data protection authorities. Indeed, the requirements established under Article 23 of the Proposal suggest a 'technical' nature of these authorities, "legally distinct from, and functionally independent of any provider of data sharing services or entity included in the register of recognised data altruism organizations".
207. In this regard, the role of the data protection supervisory authorities seems limited - under Chapter III - to having a mere exchange of information with the competent authority, and - under Chapter IV- to cooperate with the latter and provide an opinion or decision regarding questions requiring an assessment of compliance with the GDPR, at the request of the competent authority. Moreover, how and to what extent data protection authorities will interact with such competent authorities is not defined by the Proposal, as well as which financial and human resources have been envisaged to allow data protection authorities to carry out the tasks required by such interaction.
208. The EDPB and the EDPS notice that many provisions of the Proposal, whose supervision is assigned to competent authorities, designated pursuant to Article 12 and 20, are related to the protection of personal data. Bearing this in mind, **the EDPB and the EDPS underline that the competences and powers of the independent supervisory authorities shall be fully respected as they are entrusted with the responsibility to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data , as established under the GDPR and EUDPR, in line with Article 16 TFEU and Article 8 of the Charter and in accordance with the relevant case law of the Court of Justice of the European Union⁹⁵.** Considering the above, the EDPB and the EDPS recommend that the Proposal explicitly acknowledge that, inasmuch as personal data is involved, data protection authorities are the main competent authorities for the monitoring of the compliance with the provisions under Chapter III and IV of the Proposal, in consultation with other relevant sectorial authorities, when necessary. As already underlined, adequate resources should

⁹⁵ See, among others, Judgment of the ECJ of 9 March 2010, *European Commission v Federal Republic of Germany*, in case C-518/07 available at: <http://curia.europa.eu/juris/liste.jsf?language=en&num=C-518/07>. In its judgment of 9 March 2010, the Court considered that DPAs should be free from any external influence, whether direct or indirect. The mere risk of an external influence is sufficient to conclude that the DPA cannot act with complete independence.

be provided to these authorities to allow them to effectively and efficiently perform the necessary supervision.

3.7.2 Article 24: complaints; Article 25: right to effective judicial remedy

209. The EDPB and the EDPS notice that Article 24 provides that “*Natural and legal persons shall have the right to lodge a complaint with the relevant national competent authority against a provider of data sharing services or an entity entered in the register of recognised data altruism organisations*”, but does not specify the possible content of the complaint (namely, for which violation of the Proposal). It also seems that complaints against public sector bodies or re-users referred to under Chapter II of the Proposal are not possible, not foreseen under Article 24 of the Proposal.
210. In addition, Article 25 lays down the right to effective judicial remedy by any affected natural or legal person with regard to a failure to act on a complaint lodged with the competent authority, as well as with regard to decisions of competent authorities under Articles 13, 17 and 21 (respectively, decision related to supervision on data sharing services; registration of data altruism organisations; monitoring of compliance of registered data altruism organisations).
211. The EDPB and the EDPS observe that the aforesaid provisions of the Proposal on the right to lodge a complaint to the relevant national competent authority (Article 24) and on the right to an effective judicial remedy against failure to act or decisions of aforesaid competent authority (Article 25) might increase the risk, highlighted in this opinion, of parallel and inconsistent regimes between the GDPR and the Proposal. For instance, complaints related to intermediation services which provide data subjects the availability of means to exercise the rights provided under the GDPR (see Article 9(1)(b)) would fall under the remit of the competent authorities under the Proposal. In other words, the ‘substantive law’ inconsistencies and overlaps would also ‘escalate’ into administrative and judicial proceedings’ overlaps of competences.
212. For this reason, **the EDPB and the EDPS call for a clear, unambiguous and rigorous definition of the substantive rules of the Proposal whose supervision is assigned to competent authorities, and of its monitoring mechanism, which ensures full consistency with the GDPR.**

3.7.3 Articles 26 and 27: composition and tasks of the European Data Innovation Board Expert Group

213. Chapter VI of the Proposal “*creates a formal expert group (the ‘European Data Innovation Board’) with the task of facilitating the emergence of best practices by Member States’ authorities in particular on processing requests for the re-use of data which is subject to the rights of others (under Chapter II), on ensuring a consistent practice regarding the notification framework for data sharing service providers (under Chapter III), and for data altruism (Chapter IV). In addition, the formal expert group will support and advise the Commission on the governance of cross-sectoral standardisation and the preparation of strategic cross-sector standardisation requests*”⁹⁶.

⁹⁶ Explanatory Memorandum, page 8.

214. The EDPB and the EDPS notice that the newly established European Data Innovation Board, “*consisting of the representatives of competent authorities of all the Member States, the European Data Protection Board, the Commission, relevant data spaces and other representatives of competent authorities in specific sectors*” (Article 26(1)) would be entrusted with the tasks listed under Article 27, letters (a)-(e)⁹⁷, which are also relevant having regard to the processing of personal data.
215. **The EDPB and the EDPS welcome the inclusion of the EDPB as a member of the European Data Innovation Board.** However, the EDPB and the EDPS consider that the provisions related to the European Data Innovation Board are likely to impinge, insofar as relating to the processing of personal data, on the tasks and competences of national data protection authorities and of the EDPB to protect the fundamental rights and freedoms of natural persons and to facilitate the free flow of personal data within the Union⁹⁸ (having regard in particular to the wide range of tasks entrusted to the EDPB under Article 70 of the GDPR to advise the Commission and to issue guidelines, recommendations and best practices, and to the tasks entrusted to the EDPS under Article 57 of the EUDPR).
216. Therefore, the EDPB and the EDPS recommend clarifying in the legal text that the data protection supervisory authorities established under national and Union law are the “competent authority”, insofar as the processing of personal data is concerned. In addition, it should be clear that the provision of advice to the European Commission regarding data protection matters and the development of consistent practices related to the processing of personal data do not fall within the competences attributed to the European Data Innovation Board, since article 70 GDPR explicitly confers those tasks to the EDPB.
217. **The EDPB and the EDPS also recommend, for precision and legal clarity, as well as avoidance of possible misunderstanding, renaming the European Data Innovation Board as “Commission Expert**

⁹⁷ “The Board shall have the following tasks:

(a) to advise and assist the Commission in developing a consistent practice of public sector bodies and competent bodies referred to in Article 7(1) **processing requests for the re-use of the categories of data referred to in Article 3(1);**

(b) to advise and assist the Commission in developing a consistent practice of the competent authorities in the application of **requirements applicable to data sharing providers;**

(c) to advise the Commission on the **prioritisation of cross-sector standards to be used and developed for data use and cross-sector data sharing**, cross-sectoral comparison and exchange of best practices with regards to sectoral requirements for security, access procedures, while taking into account sector-specific standardisations activities;

(d) to assist the Commission in **enhancing the interoperability of data as well as data sharing services** between different sectors and domains, building on existing European, international or national standards;

(e) to facilitate the cooperation between national competent authorities under this Regulation through capacity-building and the exchange of information, in particular by establishing methods for the efficient exchange of information relating to the notification procedure for data sharing service providers and the registration and monitoring of recognised data altruism organisations.”

⁹⁸ See for instance Article 27(a), according to which the Board shall have the task to “advise and assist the Commission in developing a consistent practice of public sector bodies and competent bodies referred to in Article 7 (1) processing requests for the re-use of the categories of data referred to in Article 3 (1);” (emphasis added)

Group on Data Governance” or similar, to better reflect the *legal status* and the *nature* of the body established under Article 26 of the Proposal.

3.7.4 Article 31: penalties for infringements of the Proposal, to be applied

218. **The Proposal does not harmonize the penalties for infringements of the Proposal (nor specifies the violations that shall be sanctioned, the fines for the infringements of its provisions, nor the authorities or bodies competent to apply such penalties), providing that “Member States shall lay down the rules on penalties applicable to infringements of this Regulation and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall notify the Commission of those rules and measures by [date of application of the Regulation] and shall notify the Commission without delay of any subsequent amendment affecting them.”**
219. The EDPB and the EDPS notice that this provision, limiting the enforceability of the Proposal (the capability to impose harmonised sanctions), and possibly also giving raise to forum-shopping for the most lenient Member State, is prejudicial to the stated aim of the Proposal to increase trust in re-use, data sharing services and data altruism.

3.7.5 Article 33: amendment to Regulation (EU) 2018/1724

220. This Article of the Proposal amends the single digital gateway regulation (Regulation (EU) 2018/1724)⁹⁹, introducing the following administrative procedures: notification as provider of data sharing services; registration as a European Data Altruism Organization. The expected outcome of which is, respectively: confirmation of the receipt of the notification, confirmation of the registration.
221. **In this regard, the EDPB and the EDPS observe that the notification and registration regime, already analysed in this Opinion, cannot replace the necessity of an appropriate legal ground for the processing of personal data under Article 6(1) of the GDPR for the lawfulness of the data processing. In other words, according to the GDPR the processing of personal data shall be lawful only if and to the extent that an adequate legal basis under Article 6(1) of the GDPR applies. The Proposal should clearly specify this aspect to avoid any ambiguity.**

Brussels, 10 March 2021

For the European Data Protection Board

The Chair

(Andrea Jelinek)

For the European Data Protection Supervisor

The European Data Protection Supervisor

(Wojciech Wiewiorowski)

⁹⁹ Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012 (Text with EEA relevance.), OJ L 295, 21.11.2018, p. 1–38.



EUROPEAN
COMMISSION

Brussels, XXX
[...](2020) XXX draft

COMMISSION IMPLEMENTING DECISION

of XXX

on standard contractual clauses between controllers and processors for the matters referred to in Article 28 (3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29 (7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council

(Text with EEA relevance)

Commented [A1]: The title is referring to 28 (3) - (4) GDPR on one side and 29 (7) EUDPR on the other side. We should align and either refer to 28(3) and (4) GDPR / 29 (3) and (4) EUDPR or to 28 (7) GDPR / 29 (7) EUDPR.

Also the title is not aligned with the one mentioned in the Annex

COMMISSION IMPLEMENTING DECISION

of XXX

on standard contractual clauses between controllers and processors for the matters referred to in Article 28 (3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29 (7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR)¹, and in particular Article 28(7) thereof,

Having regard to Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (EUDPR)², and in particular Article 29(7) thereof,

Whereas:

- (1) The concepts of controller and processor play a crucial role in the application of Regulation (EU) 2016/679 and of Regulation (EU) 2018/1725. The controller is 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. For the purpose of Regulation (EU) 2018/1725, a controller means the Union institution or body or the directorate-general or any other organisational entity 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 a specific Union act, the controller or the specific criteria for its nomination can be provided for by the Union. A processor is the natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller.
- (2) The same set of standard contractual clauses should apply in respect of the relationship between data controllers and data processors subject to Regulation (EU) 2016/679 and Regulation (EU) 2018/1725, respectively. This is justified by the fact that, in the interest of a coherent approach to personal data protection throughout the Union and the free movement of personal data within the Union the data protection rules applicable to the public sector in the Member States and the data protection rules for Union institutions, bodies, offices and agencies were aligned as far as possible between Regulation (EU) 2016/679 and Regulation (EU) 2018/1725.

¹ OJ L 119, 4.5.2016, p. 1.

² OJ L 295, 21.11.2018, p. 39.

Commented [A2]: We suggest adding "by Union law" as per the definition of controller under Article 3(8) EUDPR

Commented [A3]: These definitions do not exist in the law. We would rather suggest to refer to the notions of "controller" and "processor".

Annex 1 to the EDPB - EDPS Joint Opinion 1/2021 - Comments and suggested changes to the Draft Implementing Decision

- (3) To ensure compliance with the requirements of Regulations (EU) 2016/679 and (EU) 2018/1725, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organizational measures which meet the requirements of Regulation (EU) 2016/679 and Regulation (EU) 2018/1725 , including for the security of processing.
- (4) The processing by a processor is to be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the elements listed in Article 28(3) and (4) of Regulation (EU) 2016/679 or Article 29(3) and (4) of Regulation (EU) 2018/1725. That contract or act is in writing, including in electronic form.
- (5) In accordance with Article 28(6) of Regulation (EU) 2016/679 and Article 29(6) of Regulation (EU) 2018/1725, the controller and the processor may choose either to negotiate an individual contract containing the compulsory elements laid down in Article 28(3) and (4) of Regulation (EU) 2016/679 or Article 29(3) and (4) of Regulation (EU) 2018/1725, respectively, or to rely, in whole or in part, on standard contractual clauses adopted by the Commission pursuant to Article 28(7) of Regulation (EU) 2016/679 and Article 29(7) of Regulation (EU) 2018/1725.
- (6) The controller and processor should be free to include the standard contractual clauses laid down in this Decision in a wider contract, and to add other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses or prejudice the fundamental rights or freedoms of data subjects. Reliance on the standard contractual clauses is notwithstanding any contractual obligations of the controller and or processor to ensure respect for applicable privileges and immunities.
- (7) The standard contractual clauses should provide for both substantive and procedural rules. Moreover, in line with Article 28(3) of Regulation (EU) 2016/679 and Article 29(3) of Regulation (EU) 2018/1725, the standard contractual clauses should require the controller and processor to set out the subject matter and duration of the processing, its nature and purpose, the type of personal data concerned, as well as the categories of data subjects and the obligations and rights of the controller.
- (8) Pursuant to Article 28(3) of Regulation (EU) 2016/679 and pursuant to Article 29(3) of Regulation (EU) 2018/1725, the processor has to inform the controller immediately, if, in its opinion, an instruction of the controller infringes Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, respectively or other Union or Member State data protection provisions.
- (9) Where a processor engages another processor for carrying out specific activities, the specific requirements referred to in Article 28(2) and (4) of Regulation (EU) 2016/679 or Article 29(2) and (4) of Regulation (EU) 2018/1725 should apply. In particular, a prior written authorisation is required. Such authorisation could be specific or general. In both cases, the first processor should keep a list of other processors updated.
- (10) To fulfil the requirements of Article 46(1) Regulation (EU) 2016/679, the Commission adopted standard contractual clauses pursuant to Article 46(2)(c) Regulation (EU) 2016/679. Those clauses also fulfil the requirements of Article 28(3) and (4) of Regulation (EU) 2016/679 for data transfers from controllers subject to Regulation (EU) 2016/679 to processors outside the territorial scope of application of that Regulation or

Commented [A4]: We would suggest to explain further to which extent parties can rely only in part on SCCs and to clarify that in case SCCs are relied upon only in part, the requirements of Article 28 (3) and (4) GDPR should still be fulfilled.

Commented [A5]: We suggest to clarify that this sentence and this reference to applicable privileges and immunities is relevant in the framework of SCCs under Regulation 2018/1725.

Commented [A6]: We suggest including "prior written authorisation of the controller" to make it explicit that in line with the GDPR and EUDPR this is always the prior authorisation of the controller.

Commented [A7]: We would suggest to use the wording "initial processor" in line with the terminology in GDPR and EUDPR. Moreover, where a reference is made to the "list of other processors", it should be clear that it refers also to sub-processor.

Commented [A8]: See comment in the Joint Opinion on the scope and interaction with the transfer SCCS.

Annex 1 to the EDPB - EDPS Joint Opinion 1/2021 - Comments and suggested changes to the Draft Implementing Decision

- from processors subject to Regulation (EU) 2016/679 to sub-processors outside the territorial scope of that Regulation.
- (11) Third parties should be able to become a party to the standard contractual clauses throughout the life cycle of the contract.
- (12) The [operation] of the standard contractual clauses should be evaluated in the light of experience, as sub-part of the periodic evaluation of Regulation (EU) 2016/679 referred to in Article 97 of that Regulation.
- (13) [PLACEHOLDER: The European Data Protection Supervisor and the European Data Protection Board were consulted in accordance with Article 42(1) and (2) of Regulation (EU) 2018/1725 and delivered a [joint opinion] on [...]³, which has been taken into consideration in the preparation of this Decision.]
- (14) [PLACEHOLDER: The measures provided for in this Decision are in accordance with the opinion of the Committee established under Article 93 of Regulation (EU) 2016/679 and Article 96(2) of Regulation (EU) 2018/1725.]

HAS ADOPTED THIS DECISION:

Article 1

The standard contractual clauses as set out in the Annex fulfil the requirements for contracts between the controller and the processor in Article 28(3) and (4) of Regulation (EU) 2016/679 and of Article 29(3) and (4) of Regulation (EU) 2018/1725.

Article 2

The standard contractual clauses as set out in the Annex may be used in contracts between a controller and a processor who processes personal data on its behalf, where the controller and the processor are subject to Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

Commented [A9]: In terms of wording, we would prefer referring to the “implementation of the use of SCCs” or “practical application” as mentioned in Art. 3 below.

Commented [A10]: We would also recommend to add a reference to the review process of Art. 97 EUDPR.

Article 3

The Commission shall evaluate the practical application of the standard contractual clauses set out in the Annex on the basis of all available information as part of the periodic evaluation provided for in Article 97 of Regulation (EU) 2016/679.

Commented [A11]: See comment in the text of the Joint Opinion.

Article 4

This Decision shall apply from ...

Done at Brussels,

*For the Commission
Ursula VON DER LEYEN
The President*

³



Commented [A1]: The title is not perfectly aligned with the one of the implementing Decision. See the comment made under the Draft implementing act.

ANNEX

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

- (a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and Article 29(3) and (4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data.
- (b) The data controllers and data processors listed in Annex I [‘The Parties’] have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and Article 29 (3) and (4) Regulation (EU) 2018/1725, which require the processing by a processor(s) to be governed by a contract or other legal act under Union or Member State law.
- (c) These Clauses apply with respect to the processing of personal data as specified in Annex II [Description of the Processing(s)].
- (d) Annexes I to VII form an integral part of the Clauses.

Commented [A2]: To ensure consistency with the wording of art. 28(3) of the GDPR.

Clause 2

Invariability of the Clauses

- (a) The Parties undertake not to modify the Clauses.
- (b) This does not prevent the Parties to include the standard contractual clauses laid down in this Clauses in a wider contract, and to add other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses or prejudice the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

- (a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

Annex 2 to the EDPB - EDPS Joint Opinion 1/2021 - Comments and suggested changes to the Draft SCCs

- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 respectively.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 respectively or prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

In the event of a conflict between these Clauses and the provisions of any other agreement between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5

[DOCKING CLAUSE] – Optional

- (a) Any entity which is not a Party to the Clauses may, with the agreement of all the Parties, accede to these Clauses at any time either as a data controller or as a data processor by completing Annex I [list of Parties], Annex II [description of the processing(s)] and Annex III [technical and organisational measures].
- | (b) Once Annex I is completed and signed and Annexes II and III are completed, the acceding entity shall be treated as a Party to these Clauses and shall have the rights and obligations of a data controller or a data processor, in accordance with its designation in Annex I.
Commented [A3]: In order to ensure that the Annexes are completed before the new entity accedes to the Clauses.
- (c) The acceding entity shall have no rights or obligations arising from the period prior to the date of signing Annex I.

EN

EN

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, and in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the data controller, are specified in Annex II.

Clause 7

Obligations of the Parties

- (a) The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. Such instructions are specified in Annex IV. Subsequent instructions may also be given by the data controller throughout the duration of the processing of personal data. Such instructions shall always be documented.
- (b) The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

Commented [A4]: Please see the remarks made in the Joint Opinion concerning this clause.

7.1. Purpose limitation

The data processor shall process the personal data on behalf of the data controller and only for the specific, explicit and legitimate purpose(s) of the processing specified by the data controller, as set out in Annex II [Details of the processing operation].

Commented [A5]: For the sake of clarity, the EDPB and the EDPS recommend aligning the wording on Article 5 (1) (b) GDPR.

7.2. Erasure or return of data

Processing by the data processor shall only take place for the duration specified in Annex II.

Upon termination of the provision of personal data processing services or termination pursuant to Section III Clause 10, the data processor shall at the choice of the controller

Commented [A6]: For the avoidance of doubt, the EDPB and the EDPS recommend specifying that the purposes of the processing are set by the data controller.

[OPTION 1] delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so /

Commented [A7]: The EDPB/EDPS suggest further clarifying that the purposes of processing are set by the controller in accordance with Article 28 (3) GDPR.

[OPTION 2] return all the personal data to the data controller

Commented [A8]: We suggest that a reference to the storage limitation principle should be added in this clause.

and delete existing copies unless Union or Member State law requires storage of the personal data.

Commented [A9]: We suggest the inclusion of this wording ("at the choice of the controller") in order to more closely match the wording of Article 28 (3) (g) GDPR.

7.3. Security of processing

Commented [A10]: The EDPB and the EDPS suggest replacing "certify" with "demonstrate" to avoid any confusion with certification.

Commented [A11]: Please see the comment made on this point in the Joint Opinion.

Annex 2 to the EDPB - EDPS Joint Opinion 1/2021 - Comments and suggested changes to the Draft SCCs

- (a) The processor shall, together with the controller, to which they shall provide assistance as necessary, assess and implement the appropriate level of security, taking into account the risks entailed by the processing for the rights and freedoms of the persons whose personal data are processed, the nature of the personal data, the nature, scope, context and purposes of the processing as well as the state of the art and the cost of implementation of the identified security measures. The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data, including protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access. The data processor shall implement the technical and organisational measures specified in Annex III to ensure the security of the personal data, including protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (personal data breach). In assessing the appropriate level of security, they shall in particular take due account of the risks involved in the processing, the nature of the personal data and the nature, scope, context and purposes of processing.

In the event of a personal data breach concerning data processed by the data processor, it shall notify the data controller without undue delay and at the latest within [NUMBER OF HOURS] after the data processor becoming aware of the data breach at the latest within 48h after having become aware of the breach. Such notification shall contain the details of a contact point where more information concerning the personal data breach can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and data records concerned), its likely consequences and the measures taken or proposed to be taken to mitigate its possible adverse effects. Where, and insofar as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall be provided as it becomes available without undue further delay.

- (b) The data processor shall cooperate in good faith with and assist the data controller in any way necessary to enable the data controller to notify, where relevant, the competent data protection authority and the affected data subjects, taking into account the nature of processing the personal data breach and the information available to the data processor.
- (c) The data processor shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contractual clauses. The data processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.4. Documentation and compliance

- (a) The Parties shall be able to demonstrate compliance with these Clauses.
- (b) The data processor shall deal promptly and properly with all reasonable inquiries from the data controller that relate to the processing under these Clauses.

The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations set out in these Clauses and that are stemming directly from Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 and at the data controller's request, allow for and contribute to reviews of data files, systems, and documentation, and allow for and contribute to or of audits of the

Commented [A12]: We believe that the definition of data breach has in any case to be brought in line with the text of art. 4 (12) of the GDPR and the EUDPR: "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".

Commented [A13]: We would suggest to reorganise and reword this paragraph.

The first obligation is to identify measures upon a risk-based approach and assist the controller. Then the clauses might want to specify those measures the controller has already identified. Yet, the obligation for the identification of measures based on the risks remain also incumbent also on the processor independently from the conclusions reached by the controller.

A possible text, completely replacing what is proposed ("The data processor ... purpose of processing") is proposed directly in the text.

Commented [A14]: Please see the remarks made in the Joint Opinion concerning this clause

Commented [A15]: wording aligned with Art. 33 (4) GDPR.

Commented [A16]: The EDPB and EDPS suggest that as there is a specific Clause on data breach notification these developments might not be needed in this Clause but would be better placed in Clause 9.

Commented [A17]: The EDPB and EDPS do not see the need for such specification which is not present in the GDPR

Commented [A18]: To align with the wording of Art. 33 (3) (a) and 34 (2) GDPR.

Commented [A19]: Editorial suggestion for consistency with the rest of the text.

Commented [A20]: The term "reasonable" is likely to raise a lot of questions and is subject to interpretation. In addition, stating that the processor shall deal with reasonable inquiries only also seems in contradiction with the obligation stated in the subsequent paragraph that the processor shall make available to the controller all information necessary to demonstrate compliance in accordance with Art. 28 (3) (h) GDPR.

Commented [A21]: Such addition seems necessary to better reflect what may be subject to an audit.

Commented [A22]: The wording suggests that only a review of audit would be allowed. The proposal aims to reflect the provisions of Art. 28 (3) (h) GDPR that are relevant in this context.

Annex 2 to the EDPB - EDPS Joint Opinion 1/2021 - Comments and suggested changes to the Draft SCCs

processing activities covered by these Clauses, in particular if there are indications of non-compliance.

- (c) The data controller may choose to conduct the audit by itself, to mandate, at its own cost, an independent auditor or to rely on an independent audit mandated by the data processor. Where the data processor mandates an audit, it has to bear the costs of the independent auditor. Audits may also include inspections at the premises or the physical facilities of the data processor and shall be carried out with reasonable notice.
- (d) The data processor and data controller shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority on request.

7.5. Special categories of personal data

If the processing involves i) personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, ii) genetic data, iii) or biometric data for the purpose of uniquely identifying a natural person, iv) data concerning health or v) data concerning a person's sex life or sexual orientation, or vi) data relating to criminal convictions and offences (special categories of data), the data processor shall apply specific restrictions and/or the additional safeguards laid down in Annex V.

7.6. Use of sub-processors

- (a) **OPTION 1 SPECIFIC PRIOR AUTHORISATION:** The data processor shall not subcontract any of its processing operations performed on behalf of the data controller under these Clauses to a sub-processor, without its prior specific written agreement. In order to make the assessment and the decision whether to authorise sub-contracting, the data processor shall provide the data controller with all necessary information on the intended sub-processor, including on their locations, the processing activities they will be carrying out and on any safeguards and measures to be implemented. The data processor shall submit the request for specific authorisation at least [SPECIFY TIME PERIOD] prior to the engagement of the concerned sub-processor. The list of sub-processors already authorised by the data controller can be found in Annex VI. The Parties shall keep Annex VI up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION The data processor has the data controller's general authorisation for the engagement of sub-processors. The list of sub-processors the data processor intend to engage is be found in Annex VI. The data processor shall specifically inform in writing the data controller of any intended changes of that list through the addition or replacement of sub-processors at least [SPECIFY TIME PERIOD] in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). In order to make the assessment and the decision whether to authorise sub-contracting, the data processor shall provide the data controller with all necessary information on the intended sub-processor, including on their locations, the processing activities they will be carrying out and on any safeguards and measures to be implemented. The Parties shall keep Annex VI up to date.

- (b) Where the data processor engages a sub-processor for carrying out specific processing activities (on behalf of the data controller), it shall do so by way of a contract which imposes on the sub-processor the same obligations as the ones imposed on the data processor under these Clauses. and these should be binding as a matter of EU or

Commented [A23]: This part seems unnecessary, as the processor must in any case participate in audits or inspections, regardless of the (non)existence of indications of non-compliance. Also, this might be misunderstood to restrict the statutory audit right.

Commented [A24]: The right of audit of the controller should not be limited to premises of the processor but should also cover the places where the processing is carried out. This may be the case of the processor's physical facilities.

Commented [A25]: The EDPB and EDPS wonder whether imposing a requirement for the controller to give the processor reasonable notice applies in each and every case.

Commented [A26]: We suggest referring to "genetic data" separately like Article 9 GDPR does.

Commented [A27]: We think this mirrors the wording of the GDPR more accurately.

Commented [A28]: It should be specified that these specific restrictions or specific safeguards should be in accordance with the specific instructions or guarantees requested by the controller. The processor should not decide on its own what such safeguards can be in line with Article 28 (3) GDPR which imposes compliance with controller instructions.

Commented [A29]: We would recommend to include this new sentence to reflect the following recommendation from the EDPB C-P GLs, p. 39, par 148: "*In order to make the assessment and the decision whether to authorise subcontracting, a list of intended sub-processors (including per each: their locations, what they will be doing and proof of what safeguards have been implemented) will have to be provided to the data controller by the processor*"⁵⁴. *This information is needed, so that the controller can comply with the accountability principle in Article 24 and with provisions of Articles 28(1), 32 and Chapter V of the GDPR.*"

Commented [A30]: Therefore, the EDPB and the EDPS call on the Commission to provide for an obligation to inform data subjects of their right to request the restriction of the processing of their data.

Commented [A31]: We suggest that it should be specified that the time period must be long enough to ensure the controller has a meaningful right to object.

Commented [A32]: We would recommend to include this new sentence to reflect the following recommendation from the EDPB Guidelines on the concepts of controller and processor in the GDPR, p. 39, par 148: "*In order to make the assessment and the decision whether to authorise subcontracting, a list of intended sub-processors (including per each: their locations, what they will be doing and proof of what safeguards have been implemented) will have to be provided to the data controller by the processor.*" ... [1]

Commented [A33]: We are of the opinion that the legal consequences of an objection to a new sub-processor should be further detailed in the contract. In particular, it has to be clear that in the case of an objection the processor shall not engage the sub-processor. ... [2]

Commented [A34]: In line with Art. 28 (4) GDPR and Art. 29 (4) EUDPR, obligations shall be imposed on the other processor by way of contract or other legal act under Union or Member State law.

Annex 2 to the EDPB - EDPS Joint Opinion 1/2021 - Comments and suggested changes to the Draft SCCs

- Member State law. The data processor shall ensure that the sub-processor complies with the obligations to which the data processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 / Regulation (EU) 2018/1725.
- (c) The data processor shall provide, at the data controller's request, a copy of such a sub-processor agreement and subsequent amendments to the data controller.
- (d) The data processor shall remain fully responsible to the data controller for the performance of the sub-processor's obligations under its contract with the data processor. The data processor shall notify the data controller of any failure by the sub-processor to fulfil its obligations under that contract.
- (e) The data processor shall agree a third party beneficiary clause with the sub-processor whereby - for instance in the event of bankruptcy of the data processor - the data controller shall be a third party beneficiary to the sub-processor contract and shall have the right to enforce the contract against the sub-processor, including where applicable by instructing the sub-processor to erase or return the personal data.
- (f) Prior to processing, the data processor shall inform the sub-processor of the identity and contact details of all controllers for which the sub-processor processes personal data.

7.7. International transfers

- (a) Any transfer of data to a third country or an international organisation by the data processor shall be undertaken only on the basis of documented instructions from the data controller listed in Annex IV or a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679.
- (b) The data controller agrees that where the data processor engages a sub-processor in accordance with Clause 7.6. for carrying out specific processing activities (on behalf of the data controller) in a third country or international organisation and those processing activities involve transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor may use standard contractual clauses adopted by the Commission on the basis of Article 46(2) of Regulation (EU) 2016/679 in order to comply with the requirements of Chapter V of Regulation (EU) 2016/679, provided the conditions for the use of those clauses are met and the sub-processor is able to comply with all stipulations of those clauses.

Clause 8

Data subject rights

- (a) The data processor shall promptly notify the data controller about any request received directly from the data subject. It shall not respond to that request itself, unless and until it has been authorised to do so by the data controller.
- (b) Taking into account the nature of the processing, the data processor shall assist by appropriate technical and organisational measures, insofar as this is possible, the data controller in fulfilling its obligations laid down in Chapter III of the GDPR, in particular-to respond to data subjects' requests for the exercise of their rights, namely:
- (1) the right to be informed when personal data are collected from the data subject,

Commented [A35]: The EDPB and the EDPS suggest the inclusion of this clause. A similar clause was also present in the Danish and Slovenian SCCs.

Commented [A36]: The EDPB and EDPS are of the opinion that this information would need to be provided. This should also be specified in the Annexes as parties should be requested to provide the information in the annexes..

Commented [A37]: Please see the remarks made in the Joint Opinion concerning this clause.

Commented [A38]: We suggest the inclusion of references to Regulation 2018/1725. When EUIs engage processors and allow transfers from processor of EUIs to recipients a third country or international organisation, references only to GDPR are not correct, rather references to the EUDPR should also be made.

Commented [A39]: We suggest the inclusion of this wording to ensure alignment with the wording of Article 28 (3) (a) GDPR.

Commented [A40]: The use the SCCs – even if the conditions for their use are met – is not sufficient if the subprocessor is not able to comply with them. Otherwise, an onward transfer to a third country which normally would require supplementary measures might be permitted without supplementary measures.

Commented [A41]: Please see the remarks made in the Joint Opinion concerning this clause.

Commented [A42]: The proposed changes aim at bringing the text in line with the text of the GDPR and also clarifying that the assistance is not always linked to a request from the data subject (for instance for items 1, 2 and 10 of the list).

Annex 2 to the EDPB - EDPS Joint Opinion 1/2021 - Comments and suggested changes to the Draft SCCs

- (2) the right to be informed when personal data have not been obtained from the data subject,
- (3) the right of access by the data subject,
- (4) the right to rectification,
- (5) the right to erasure ('the right to be forgotten'),
- (6) the right to restriction of processing,
- | (7) the notification obligation regarding rectification or erasure of personal data or restriction of processing,
- | (8) the right to data portability,
- | (9) the right to object,
- | (10) the right not to be subject to a decision based solely on automated processing, including profiling.
- (c) In addition to the data processor's obligation to assist the data controller pursuant to Clause 8(b), the data processor shall furthermore assist the data controller in ensuring compliance with the following obligations, taking into account the nature of the processing and the information available to the data processor:
- | (1) The obligation to notify a personal data breach to the competent supervisory authority [INDICATE THE NAME OF THE COMPETENT DPA] without undue delay after having become aware of it, (unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);
- | (2) the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;
- | (3) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;
- | (4) the obligation to consult the competent supervisory authority [INDICATE THE NAME OF THE COMPETENT DPA] prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.
- (d) The Parties shall set out in Annex VII the appropriate technical and organisational measures by which the data processor is required to assist the data controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the data processor shall cooperate in good faith with and assist the data controller in any way necessary for the data controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, taking into account the nature of processing and the information available to the processor.

Commented [A43]: The EDPB and the EDPS invite the European Commission to include a point referring to the obligations of security under Article 32 GDPR and the obligations of security and confidentiality under Articles 33, 36, 37, 38, 41 EU DPR (to reflect the wording of Article 28 GDPR and Article 29 EU DPR).

Please also see paragraph 49 of the Joint Opinion.

Commented [A44]: Please see the remarks made in the Joint Opinion concerning this clause.

Commented [A45]: The EDPB and the EDPS are not sure to fully understand the distinction between Annexes III and VII.

To distinguish from Annex III, Annex VII could provide details on how the processor is to provide assistance to the controller to comply:

- with controller's obligations to respond to requests for exercising data subject's rights laid down in Chapter III of the GDPR and Chapter III of the EUDPR and
- with controller's obligations under Arts. 32 to 36 GDPR and Arts. 33 to 41 EUDPR

Commented [A46]: The requirements to notify a competent authority (and name the competent authority), which are now addressed under clause 7.3, letter (a), clause 8 (c) (1) and clause 9 could be addressed under one clause (i.e. clause 9) in order to avoid repetition.

Commented [A47]: The EDPB and EDPS do not see the need for such specification which is not present in the GDPR

- (a) In accordance with Clause 8(b) the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, where relevant [INDICATE THE NAME OF THE COMPETENT DPA]. The data processor shall be required to assist in obtaining in particular the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679 or under Articles 34(3) Regulation (EU) 2018/1725, shall be stated in the data controller's notification:
- (1) The nature of the personal data **breach** including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
 - (2) the likely consequences of the personal data breach;
 - (3) the measures taken or proposed to be taken by the data controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
- (b) The Parties shall set out in Annex VII all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

SECTION III – FINAL PROVISIONS

Clause 10

Termination

- (a) Without prejudice to any provisions of Regulation (EU) 2016/679 / Regulation (EU) 2018/1725, in the event that the data processor is in breach of its obligations under these Clauses, the data controller may instruct the data processor to temporarily suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The data processor shall promptly inform the data controller in case it is unable to comply with these Clauses, for whatever reason.
- (b) The data controller shall be entitled to **terminate these Clauses** where:
- (1) the processing of personal data by the data processor has been temporarily suspended by the data controller pursuant to point (a) and compliance with these Clauses is not restored within a reasonable time and in any event within one month;
 - (2) the data processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 / Regulation (EU) 2018/1725;
 - (3) the data processor fails to comply with a binding decision of a competent court or the competent supervisory authority [INDICATE THE COMPETENT DPA] regarding its obligations under these Clauses or under Regulation (EU) 2016/679 / Regulation (EU) 2018/1725.

Commented [A48]: Letter (c) is the correct reference.

Commented [A49]: Corresponding to wording of Art. 33 (3) GDPR.

Commented [A50]: The EDPB and the EDPS are of the view that the European Commission should make clear that in case of termination of the Clauses the provisions of Clause 7.2 (Erasure or return of personal data) apply.

Commented [A51]: In the view of the EDPB/EDPS, it is not needed in this context to explicitly request the parties to name the competent SA.

ANNEX I LIST OF PARTIES

Commented [A52]: Please see the remarks made in the Joint Opinion concerning this Annex.

Data controller(s): *[Identity and contact details of the data controller(s), and, where applicable, of the data controller's representative in the Union designated pursuant to Article 27 Regulation (EU) 2016/679]*

1. Name: ...

Address: ...

Contact person's name, position and contact details: ...

Signature and accession date: ...

2.

...

Data processor(s): *[Identity and contact details of the data processor(s)]*

1. Name: ...

Address: ...

Contact person's name, position and contact details: ...

Signature and accession date: ...

2.

...

Annex 2 to the EDPB - EDPS Joint Opinion 1/2021 - Comments and suggested changes to the Draft SCCs

ANNEX II: DESCRIPTION OF THE PROCESSING

Purpose(s) for which the personal data is processed on behalf of the controller

Duration of the processing

Categories of data subjects whose personal data is processed

Categories of personal data processed

Special categories of personal data processed (if applicable)

[Record(s) of processing]

Place of storage and processing of data

.....

.....

Subject-matter of the processing

.....

Commented [A53]: The EDPB and EDPS suggest that the European Commission add some explanatory text on Annex 2, similar to the one that was included in the SCCs prepared by the Danish SA and the Slovenian SA. This text should, more specifically, require the parties to include a sufficiently detailed description of the categories of personal data. For instance, the explanatory text included in the aforementioned SCCs included a request to describe the type of personal data being processed, with some examples, and the note that the description should be made in the most detailed possible manner and in any circumstance the types of personal data must be specified further than merely “personal data” or “Article 9 / 10 data”.

Commented [A54]: The EDPB and the EDPS do not understand what this means and therefore suggest either deletion or clarification.

Commented [A55]: The EDPB and the EDPS suggest adding a clarification as to what “place” means – e.g. just the country or the exact names and addresses of the facilities where the personal data will be processed.

Commented [A56]: We suggest to request the parties to detail the subject matter of the processing in the Annex in order to be in line with the wording of Article 28 (3) GDPR.

EN

EN

**ANNEX III TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING
TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY
OF THE DATA**

| *Description of the technical and organisational [security] measures implemented by the data processor(s)*

Commented [A57]: In our view, this should be deleted, since now this list includes all measures, not only the security-related ones.

| [TAKING INTO ACCOUNT THE NATURE, SCOPE, CONTEXT AND PURPOSES OF THE PROCESSING ACTIVITY AS WELL AS THE RISK FOR THE RIGHTS AND FREEDOMS OF NATURAL PERSONS, DESCRIBE ELEMENTS THAT ARE ESSENTIAL TO [THE ENSURE AN ADEQUATE] LEVEL OF SECURITY]

Commented [A58]: Clarification.

Where necessary:

[DESCRIBE REQUIREMENTS FOR PSEUDONYMISATION AND ENCRYPTION OF PERSONAL DATA]

[DESCRIBE REQUIREMENTS FOR ENSURING ONGOING CONFIDENTIALITY, INTEGRITY, AVAILABILITY AND RESILIENCE OF PROCESSING SYSTEMS AND SERVICES]

[DESCRIBE REQUIREMENTS FOR THE ABILITY TO RESTORE THE AVAILABILITY AND ACCESS TO PERSONAL DATA IN A TIMELY MANNER IN THE EVENT OF A PHYSICAL OR TECHNICAL INCIDENT]

[DESCRIBE REQUIREMENTS FOR PROCESSES FOR REGULARLY TESTING, ASSESSING AND EVALUATING THE EFFECTIVENESS OF TECHNICAL AND ORGANISATIONAL MEASURES FOR ENSURING THE SECURITY OF THE PROCESSING]

| [DESCRIBE REQUIREMENTS FOR USERS IDENTIFICATION AND AUTHORISATION]
[DESCRIBE REQUIREMENTS FOR THE PROTECTION OF DATA DURING TRANSMISSION]

[DESCRIBE REQUIREMENTS FOR THE PROTECTION OF DATA DURING STORAGE]

[DESCRIBE REQUIREMENTS FOR PHYSICAL SECURITY OF LOCATIONS AT WHICH PERSONAL DATA ARE PROCESSED]

[DESCRIBE REQUIREMENTS FOR EVENTS LOGGING]

[DESCRIBE REQUIREMENTS FOR SYSTEM CONFIGURATION, INCLUDING DEFAULT CONFIGURATION]

[DESCRIBE REQUIREMENTS FOR INTERNAL IT AND IT SECURITY GOVERNANCE AND MANAGEMENTS]

[DESCRIBE REQUIREMENTS FOR CERTIFICATION / ASSURANCE OF PROCESSES AND PRODUCTS]

Annex 2 to the EDPB - EDPS Joint Opinion 1/2021 - Comments and suggested changes to the Draft SCCs

[DESCRIBE REQUIREMENTS FOR DATA AVOIDANCE AND MINIMISATION]

[DESCRIBE REQUIREMENTS FOR DATA QUALITY]

[DESCRIBE REQUIREMENTS FOR DATA RETENTION]

[DESCRIBE REQUIREMENTS FOR ACCOUNTABILITY]

[DESCRIBE REQUIREMENTS FOR DATA PORTABILITY AND DATA DISPOSAL]

Commented [A59]: This term is not used in the GDPR. We wonder whether it has a meaning that goes beyond data minimisation as described in Article 25 (1) GDPR. If so, the term should be explained; if not, it should be deleted.

Commented [A60]: This term is not used in the GDPR. We wonder whether it has a meaning that goes beyond data portability as described in Article 20 GDPR. If so, the term should be explained; if not, it should be deleted.

ANNEX IV: INSTRUCTIONS FROM THE DATA CONTROLLER CONCERNING THE PROCESSING OF PERSONAL DATA

ANNEX V: SPECIFIC RESTRICTIONS AND/OR ADDITIONAL SAFEGUARDS CONCERNING DATA OF SPECIAL CATEGORY

For special categories of personal data processed mentioned in Annex II restrictions or safeguards applied such as:

access restrictions,

keeping a record of access to the data,

restrictions of the purposes for which the information may be processed,

additional security measures (e.g. strong encryption for transmission),

requirement of specialised training for staff allowed to access the information

Commented [A61]: The term “data” seems to be more appropriate unless there is a specific reason why the term “information” has been chosen; in case of a specific reason, it should be explained.

ANNEX VI: LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

Name (full legal name):

Company number:

Address:

Description of the processing (in case several sub-processors are authorised, including a clear delimitation of responsibilities):

Place(s) of processing:

[To be completed for every authorised sub-processor]

Commented [A62]: We suggest adding the introduction and the following paragraph in order to remind the parties of the requirements stipulated in the SCCs and the law.

The controller will need approve the use of sub-processors. The processor is not entitled – without the express written consent of the controller – to engage a sub-processor for any other processing than the agreed processing or to have another sub-processor perform the described processing.

Commented [A63]: Just like with regard to the term in Annex II, we suggest adding a clarification as to what “place” means – e.g. just the country or the exact names and addresses of the facilities where the personal data will be processed.

Commented [A64]: As already mentioned in the Joint Opinion itself, the EDPS and EDPB are of the opinion that it is of utmost importance that the Annexes to the SCCs delimit with absolute clarity the roles and responsibilities of each of the parties in each relationship and with regard to each processing activity. We therefore suggest including further details on the authorised sub-processors and their activities, also reflecting the following recommendation from the EDPB C-P GLs, para. 148:

“In order to make the assessment and the decision whether to authorise subcontracting, a list of intended subprocessors (including per each: their locations, what they will be doing and proof of what safeguards have been implemented) will have to be provided to the data controller by the processor. This information is needed, so that the controller can comply with the accountability principle in Article 24 and with provisions of Articles 28(1), 32 and Chapter V of the GDPR.”

Commented [A65]: Similar to Annex III, we suggest adding the requirements to be covered in this Annex. As correctly filling out this Annex might be challenging to the parties, we suggest adding examples of possible measures or detailed descriptions of the expected assistance.

Page 5: [1] Commented [A32]**Author**

We would recommend to include this new sentence to reflect the following recommendation from the EDPB Guidelines on the concepts of controller and processor in the GDPR, p. 39, par 148: "*In order to make the assessment and the decision whether to authorise subcontracting, a list of intended subprocessors (including per each: their locations, what they will be doing and proof of what safeguards have been implemented) will have to be provided to the data controller by the processor. This information is needed, so that the controller can comply with the accountability principle in Article 24 and with provisions of Articles 28(1), 32 and Chapter V of the GDPR.*"

Page 5: [2] Commented [A33]**Author**

We are of the opinion that the legal consequences of an objection to a new sub-processor should be further detailed in the contract. In particular, it has to be clear that in the case of an objection the processor shall not engage the sub-processor.



**EDPB - EDPS Joint Opinion 1/2021
on the European Commission's
Implementing Decision on
standard contractual clauses
between controllers and
processors**

for the matters referred to in Article 28 (7)
of Regulation (EU) 2016/679 and Article 29
(7) of Regulation (EU) 2018/1725

TABLE OF CONTENTS

1	Background.....	3
2	Scope of the opinion	4
3	General reasoning regarding the Draft Decision and the Draft SCCs	4
3.1	General comments.....	4
3.2	Explanation of the methodology applied and structure of the document.....	5
4	Analysis of the Draft Decision and its Annex.....	5
4.1	Main comments on the Draft Decision.....	5
4.1.1	On the scope of the Decision and on the articulation with the other set of Draft SCCs on transfers	5
4.2	Main comments on the Annex to the Commission implementing decision.....	6
4.2.1	Purpose and scope (Clause 1 of the Draft SCCs).....	6
4.2.2	Invariability (Clause 2 of the Draft SCCs)	7
4.2.3	Docking clause (Clause 5 of the Draft SCCs)	7
4.2.4	Obligations of the Parties (Clause 7 of the Draft SCCs)	7
4.2.5	Data Subject rights (Clause 8 of the Draft SCCs).....	9
4.2.6	Annexes to the Draft SCCs	10

The European Data Protection Board and the European Data Protection Supervisor

Having regard to Article 42(2) of the Regulation 2018/1725 of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC ("EUDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

HAVE ADOPTED THE FOLLOWING JOINT OPINION

1 BACKGROUND

1. In the context of the relationship between a controller and a processor, or processors, for the processing of personal data, the Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or "GDPR") establishes, in its Article 28, a set of provisions with respect to the setting up of a specific contract between the parties involved, and mandatory provisions that should be incorporated in it.
2. According to Article 28 (3) GDPR, the processing by a processor shall be governed by a contract or other legal act under Union or Member State law that is binding on the processor with regard to the controller, setting out a set of specific aspects to regulate the contractual relationship between the parties. These include the subject-matter and duration of the processing, its nature and purpose, the type of personal data and categories of data subjects, among others. Article 28 (4) provides for additional requirements where a processor engages another processor for carrying out specific processing activities on behalf of the controller.
3. Under Article 28 (6) GDPR, without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred in paragraphs (3) and (4) of Article 28 GDPR may be based, wholly or in part, on standard contractual clauses. These standard contractual clauses are to be adopted for those matters referred to in paragraphs (3) and (4).
4. Article 28 (7) GDPR provides that the Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 93(2).
5. The EUDPR lays down rules relating to the protection of natural persons with regard to the processing of personal data by the Union institutions and bodies and rules relating to the free movement of personal data between them or to other recipients established in the Union.
6. Article 29 (3), (4) and (7) of the EUDPR contain similar requirements as the ones included in Article 28 (3), (4) and (7) of the GDPR. This is justified by the fact that, in the interest of a coherent approach to

¹ References to "Member States" made throughout this opinion should be understood as references to "EEA Member States".

personal data protection throughout the Union and the free movement of personal data within the Union, the data protection rules applicable to the public sector in the Member States and the data protection rules for Union institutions, bodies, offices and agencies were aligned as far as possible.

2 SCOPE OF THE OPINION

7. On 12 November 2020, the Commission published:
 - | a Draft Commission Implementing Decision on standard contractual clauses between controllers and processors for the matters referred to in Article 28 (3) and (4) of Regulation (EU) 2016/679 and Article 29 (7) of Regulation (EU) 2018/1725 (the “**Draft Decision**”);
 - | a draft Annex to the Commission Implementing Decision on standard contractual clauses between controllers and processors for the matters referred to in Article 28 (3) and (4) of Regulation (EU) 2016/679 and Article 29 (7) of Regulation (EU) 2018/1725 (the “**Draft SCCs**”).
8. The same day, the European Commission also published a draft Commission Implementing Decision and its Annex on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679.
9. On 12 November 2020, the European Commission requested a joint opinion of the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) on the basis of Article 42(1), (2) of Regulation (EU) 2018/1725 (EU DPR) on these two sets of draft standard contractual clauses and the respective implementing acts.
10. For the sake of clarity, the EDPB and EDPS decided to issue two separate opinions on these two sets of SCCs.
11. The scope of this opinion is thus limited to the Draft Decision and Draft SCCs between controllers and processors for the matters referred to in Article 28 (3) and (4) of the GDPR and Article 29 (3) and (4) of the EUDPR.

3 GENERAL REASONING REGARDING THE DRAFT DECISION AND THE DRAFT SCCs

3.1 General comments

12. Any set of SCCs must further specify the provisions foreseen in Article 28 GDPR and Article 29 EUDPR. The opinion of the EDPB and the EDPS aims at ensuring consistency and a correct application of Article 28 GDPR as regards the presented Draft SCCs that could serve as standard contractual clauses in compliance with Article 28 (7) GDPR and Article 29 (7) EUDPR.
13. The EDPB and the EDPS are of the opinion that clauses which merely restate the provisions of Article 28(3) and (4) GDPR and Article 29 (3) and (4) EUDPR are inadequate to constitute standard contractual clauses. The Board and EDPS have therefore decided to analyse the document in its entirety, including the appendices. In the opinion of the Board and the EDPS, a contract under Article 28 GDPR or Article 29 EUDPR should further stipulate and clarify how the provisions will be fulfilled. It is in this light that the Draft SCCs submitted to the Board and EDPS for opinion are analysed.

14. Adopted standard contractual clauses constitute a set of guarantees to be used as is, as they are intended to protect data subjects and mitigate specific risks associated with the fundamental principles of data protection.
15. The EDPB and the EDPS welcome in general the adoption of standard contractual clauses as a strong accountability tool that facilitates compliance by controllers and processors to their obligations under the GDPR and the EUDPR.
16. The EDPB already issued opinions on standard contractual clauses prepared by the Danish Supervisory Authority² and the Slovenian Supervisory Authority³.
17. To ensure a coherent approach to personal data protection throughout the Union, the EDPB and the EDPS strongly welcome the envisaged adoption of SCCs having an EU-wide effect by the Commission.
18. The same set of SCCs will indeed apply irrespective of whether this relationship involves private entities, public authorities of the Member States or EU institutions or bodies. These EU-wide SCCs will ensure further harmonisation and legal certainty.
19. The EDPB and the EDPS also welcome the fact that the same set of SCCs should apply in respect of the relationship between controllers and processors subject to GDPR and EUDPR respectively.

3.2 Explanation of the methodology applied and structure of the document

20. For the sake of clarity, the present opinion comprises (i) a core part detailing general comments the EDPB and the EDPS wish to make and (ii) and an annex where comments of a more technical nature are made directly to the Draft Decision and the Draft SCCs in order to provide some examples of possible amendments. There is no hierarchy between the general comments and the technical ones.
21. In addition, the main comments on the Draft Decision and the Draft SCCs are presented in two separate sections. Where needed, cross-references are made to ensure consistency.
22. For the sake of consistency, where needed, cross-references are also made to the EDPB - EDPS Joint Opinion 02/2021 on standard contractual clauses for the transfer of personal data to third countries.

4 ANALYSIS OF THE DRAFT DECISION AND ITS ANNEX

4.1 Main comments on the Draft Decision

4.1.1 On the scope of the Decision and on the articulation with the other set of Draft SCCs on transfers

23. Article 2 of the Draft Decision provides that “*the standard contractual clauses as set out in the Annex may be used in contracts between a controller and a processor who processes personal data on its behalf, where the controller and the processor are subject to Regulation (EU) 2016/679 or Regulation (EU) 2018/1725*”.

² Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR): https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_201914_dk_scc_en.pdf.

³ Opinion 17/2020 on the draft Standard Contractual Clauses submitted by the SI SA (Article 28(8) GDPR): https://edpb.europa.eu/our-work-tools/our-documents/opinjon-tal-bord-art-64/opinion-172020-draft-standard-contractual_en.

24. The EDPB and the EDPS are of the opinion that the current wording of this Article is source of legal uncertainty, as to the situations in which entities will be able to rely on these SCCs.
25. The EDPB and the EDPS understand that the intention of the Commission is that these SCCs are only meant to cover intra-EU situations and that these clauses should not be relied upon in case of transfer within the meaning of Chapter V. In these cases, parties should rather rely on the separate set of standard contractual clauses that has been established for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 and that is also meant at covering Article 28 (3) and 28 (4) GDPR requirements (“**transfer SCCs**”).
26. The EDPB and EDPS consider that the Draft Decision does not provide sufficient clarity to the parties and the exact scope of the Decision has to be clearly set out and detailed in a specific recital of the Draft Decision, for instance before the current Recital 10 of the Draft Decision.
27. Moreover, the Board and the EDPS are of the opinion that the current wording of Article 2 of the Draft Decision does not limit the scope to intra-EU situations as controllers or processors subject to the GDPR for a given processing activity may be established outside the EU by virtue of Article 3 (2) GDPR. It should then be clarified whether these SCCs could be relied upon in this situation.
28. Finally, the EDPB and the EDPS are rather of the opinion that the intended limitation to intra-EU situations is not justified. For example, the EDPB and EDPS do not see any reason to prevent entities from relying on these SCCs – for the sake of complying with Articles 28 (3) and 28 (4) GDPR - if one of the party is not subject to the GDPR for a given processing activity but is located in an adequate country. If the scope of the SCCs is broadened to situations involving transfers outside the EU, it should be made clear to the parties that these SCCs will provide compliance with the requirements under Article 28 (3) and 28 (4) GDPR or 29 (3) and 29 (4) EUDPR but not all the requirements deriving from the GDPR or the EUDPR, for instance on the rules related to international transfers.
29. In the view of the EDPB and the EDPS, it is also important to clearly explain in the Decision the articulation and interplay between this set of SCCs and the transfer SCCs. It should be made clear to the parties, already in the decision, that when parties intend to benefit from SCCs both under Article 28 (7) GDPR and 46 (2) c GDPR, then parties need to rely on transfer SCCs.

4.2 Main comments on the Annex to the Commission implementing decision

4.2.1 Purpose and scope (Clause 1 of the Draft SCCs)

30. **Clause 1 (a)** of the Draft SCCs specifies that the purpose of the SCCs is to ensure compliance with the GDPR and the EUDPR. The EDPB and EDPS are of the opinion that parties to the contract when signing the clauses should be able to choose to select either references to the GDPR or the EUDPR depending on the relevant Regulation applicable to their situation.
31. This way, entities using SCCs under Article 28 GDPR would have no reference to the EUDPR in their SCCs and entities relying on Article 29 EUDPR would avoid the references to the GDPR. This would contribute to bring clarity in the relations between the parties that are often less familiar with such regulations. If so, the SCCs should specify that such choice is possible and adapt the drafting of the SCCs accordingly.
32. As provided for in **Clauses 1 (b) and (c)**, and in accordance with **Clause 5** (Docking clause), several controllers and processors, listed in **Annex I**, can be parties to the SCCs for the processing specified in **Annex II**. The EDPB and EDPS believe that, in such case of multiple parties to the contract, the SCCs (and their Annexes) should require from parties to further detail and delimit the allocation of

responsibilities and indicate clearly which processing is carried out by which processor(s) on behalf of which controller(s) and for which purposes. The current formulation of these clauses of the SCCs and the Annexes may lead to confusion as to the qualification and role of each entity with respect to a given processing operation, especially given the possibility to include a docking clause.

4.2.2 Invariability (Clause 2 of the Draft SCCs)

33. According to **Clause 2 (b)** of the Draft SCCs, the parties undertake not to modify them unless additional clauses “*do not contradict, directly or indirectly*” the SCCs. To provide controllers and processors with legal certainty, the EDPB and EDPS would welcome clarifications on the type of clauses that the European Commission would consider as contradicting directly or indirectly SCCs. Such clarification could for instance indicate that clauses contradicting SCCs would be those that undermine or negatively impact the obligations in the SCCs or prevent compliance with the obligations contained in the SCCs. For example, clauses allowing processors to use the data for its own purposes would be contrary to the obligation of the processor to process personal data only on behalf of the controller, and for the purposes and by the means identified by the latter.

4.2.3 Docking clause (Clause 5 of the Draft SCCs)

34. **Clause 5** of the Draft SCCs allows, as an option, any entity to accede to the SCCs and therefore to become a new party to the contract as a controller or as a processor. As already mentioned above, the qualification and the role of such new party to the contract should appear clearly in the Annexes by requesting parties to further detail and delimit the allocation of responsibilities and indicate clearly which processing is carried out by which processor(s) on behalf of which controller(s) and for which purposes.
35. **Clause 5 (a)** makes the accession of new parties to the SCCs conditional upon the agreement of all the other parties. In order to avoid any difficulties in practice, the EDPB and EDPS would welcome a clarification on the way such agreement could be given by the other parties (whether it should be in writing or not, the deadline to provide such agreement, the information needed before agreeing). Also, the EDPB and EDPS would welcome clarification as to whether and how such agreement has to be given by all the parties, irrespective of their qualification and role in the processing.

4.2.4 Obligations of the Parties (Clause 7 of the Draft SCCs)

36. Although the title of this clause is “Obligations of the Parties”, **Clause 7 (a)** in its current form only makes reference to obligations imposed on the processor. Article 28(3) GDPR specifies that the controller/processor contract shall set out the rights, but also the obligations, of the controller. Consequently, the EDPB and EDPS suggest that a reference is added to this clause to the obligations imposed on the controller, for the purposes of completeness and enhanced clarity. For instance, the following sentence could be added before Clause 7 (a): “*The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data and is responsible for ensuring that the processing of personal data takes place in compliance with the applicable EU or Member State data protection provisions and the Clauses (including ensuring that the processing of personal data which the processor is instructed to perform relies on a legal basis pursuant to Article 6 GDPR or Article 5 EUDPR)*”.
37. Clause 7 (a) also provides that instructions should be specified in Annex IV and that subsequent instructions may also be given by the controller. The possibility for the controller to give “*subsequent instructions*” is necessary to fully implement the rights and obligations of the parties set out in the

SCCs, but is not unlimited. Any subsequent instruction should be in line with the respective rights and obligations of the parties set out in the SCCs. The EDPB and the EDPS consider that this should be clearly specified in the Clause.

38. Additionally, in order to enhance consistency with the text of 28 (3) (a) of the GDPR and Article 29 (3) (a) of the EUDPR and to include such obligation directly in the contract, the EDPB and the EDPS suggest amending the end of the first sentence of Clause 7 (a) with the following underlined wording: "*The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest*".
39. Concerning the event of unlawful instructions given by the controller, described by Article 28 (3) subparagraph 2 GDPR, the EDPB and EDPS are of the opinion that the contract between the controller and the processor should include some more precise information as to the consequences and solutions envisioned in case the processor informs the controller that, in its opinion, the instruction infringes the GDPR or other applicable data protection provisions. Therefore, the European Commission should invite the parties to include further details about the consequences of the notification of an infringing instruction in the contract (e.g. a clause on the possibility for the processor to suspend the implementation of the affected instruction until the controller confirms, amends or withdraws its instruction, a clause on the termination of the contract in case the controller persists with an unlawful instruction).
40. Concerning the options available to the controller pursuant to **Clause 7.2** relating to erasure or return of data, the EDPB and EDPS call on the European Commission to specify in the Clause itself that the controller should be able to modify the choice made at the time of signature of the contract throughout the life cycle of the contract and upon termination.
41. As a general comment on **Clause 7.3** relating to the security of processing, the EDPB and EDPS note that all obligations lie on the processor without specifying the role of the controller in particular regarding the assessment of the risk which must be performed for security measures in consideration of the purpose of the processing set by the controller. In some cases, the processor might not be aware of the exact purpose of the processing, for instance when hosting data. Therefore, and in accordance with the provision of Article 28.3 of the GDPR, the EDPB and EDPS are of the opinion that the Clause should be completed with the obligations applying with respect to the security of the processing to the controller which, in particular, has to provide all useful information to the processor to comply with the relevant requirements in this respect.
42. **Clause 7.3 (a)** of the Draft SCCs provides that the processor has 48 hours at the latest to notify the controller of a personal data breach. Such delay may be short in some situations and may also trigger confusion with the delay in which the controller has to notify the personal data breach to the SA (which starts when the controller is aware of it, i.e.; when the processor notifies him). While taking into account the requirement for the processor to notify the controller "*without undue delay*" after becoming aware of the personal data breach in accordance with Article 33.2 GDPR, the EDPB and EDPS suggest to leave the parties to provide the appropriate timeframe to meet this requirement, depending on the specific situation. The parties should thus be requested to specify in the SCCs the timeframe agreed for such notification.
43. **Clause 7.4 (c)** of the Draft SCCs provides for the possibility for the controller, in order to conduct audits, to rely on an independent auditor mandated by the processor. This provision is not foreseen

in Article 28 (3) (h) GDPR and needs to be aligned with this article which provides that the processor has to allow for and contribute to audits, including inspections, that are conducted by the controller or another auditor mandated by the controller. As such, the processor might propose an auditor, but the decision about the auditor has to be left to the controller according to Article 28 (3) (h) of the GDPR.

44. **Clause 7.4 (c)** also states that where the controller mandates an independent auditor, it shall bear the costs, and where the processor mandates an audit, it has to bear the costs of the independent auditor. As the issue of allocation of costs between a controller and a processor is not regulated by the GDPR, the EDPB and the EDPS are consequently of the opinion that any reference to the costs should be deleted from this clause.
45. With regard to **Clause 7.7** on international transfers, and more specifically concerning the situation where a processor relies on a sub-processor in a third country, the EDPB and the EDPS express the view that point (b) could be more explicit as to the possibility for these two parties to sign one single set of SCCs which aims at compliance both with Chapter V and Article 28(4) GDPR, if this is indeed the goal this clause would like to achieve, which would require further clarification. Also it should be clarified whether parties then need to rely on this set of SCCs or rather on the transfer SCCs also providing safeguards under Article 28 (3) and (4) of the GDPR.
46. Additionally, the EDPB and the EDPS would like to highlight that while **Clause 7.7 (b)** only refers to the use of the transfer SCCs, several other transfer tools could be legitimately relied upon for framing the transfers from the processor to a sub-processor in a third country, and thus suggest using a more generic formulation referring to transfer tools under Article 46 GDPR.
47. The EDPB and the EDPS also identified the need to further clarify the last part of point (b) of Clause 7.7, referring to "*the conditions for the use of*" the transfer SCCs. As this provision suggests that there may be specific conditions for the use of the transfer SCCs, there is a need to specify what these conditions are.

4.2.5 Data Subject rights (Clause 8 of the Draft SCCs)

48. The clause is currently entitled "*Data Subject rights*" but it is the opinion of the EDPB and the EDPS that the title does not reflect the content of the clause.
49. **Clauses 8 (a) and 8 (b)** of the Draft SCCs indeed refer to the processor's obligation to provide assistance with controller's obligations to respond to requests for exercising data subject's rights laid down in Chapter III of the GDPR and Chapter III of the EUDPR. However, Clauses 8 (c) and 8 (d) refer to the assistance of the processor with other types of controller's obligations, in particular under Articles 32 to 36 GDPR and Articles 33 to 41 EUDPR.
50. The EDPB and the EDPS therefore suggest to change the title of this clause to "*Assistance to the controller*" to reflect the different assistance that the processor needs to provide.
51. As an alternative, the EDPB and EDPS would recommend to the Commission to split the clause in two to distinguish between the assistance that the processor needs to provide:
 -) with controller's obligations to respond to requests for exercising data subject's rights laid down in Chapter III of the GDPR and Chapter III of the EUDPR and
 -) with controller's obligations under Articles 32 to 36 GDPR and Articles 33 to 41 EUDPR.

52. Also, Clause 8 (a) of the Draft SCCs provides that “*the data processor shall promptly notify the data controller about any request received directly from the data subject. It shall not respond to that request itself, unless and until it has been authorised to do so by the data controller*”.
53. The EDPS and EDPB are of the opinion that this clause should:
- ✓ further specify that the responses to data subjects shall be made in accordance with the controller’s instructions (e.g. on content of the response) as set out in Annex IV;
 - ✓ further specify that the scope of processor’s obligation relating to the exercise of data subject’s rights on behalf of the controller should be described and clearly set out in Annex VII.
54. **Clause 8 (c) (1)** as well as **Clause 9 (a)** require to specify the Supervisory Authority which is competent but does not envisage the case where there are several controllers parties to the contract and thus several competent supervisory authorities. Therefore, the possibility to mention several competent supervisory authorities should be added. In addition, there may be cases where the processing subject to the clauses is cross-border and a lead Supervisory Authority is to be identified as competent Supervisory Authority. This should also be reflected in Clauses 8 (c) (1) and 9 (a).
55. The EDPB and EDPS suggest that, in case processors within the EU are bound by third country laws or practices affecting the compliance with these Clauses, the Commission should assess whether an additional clause to address these cases is appropriate.

4.2.6 Annexes to the Draft SCCs

56. The SCCs are designed to be used for data processing agreements, which may involve more than one party as a controller and/or more than one party as a processor. This implies the risk that, if the Annexes are not filled out appropriately, the responsibilities of the parties are blurred. This risk increases where new parties subsequently join the contract by using the Docking Clause and/or the contract covers processing for different purposes or under different circumstances.
57. The EDPS and EDPB are of the opinion that it is of utmost importance that the Annexes to the SCCs delimit with absolute clarity the roles and responsibilities of each of the parties in each relationship and with regard to each processing activity. This is necessary for the parties to be able to determine who is processing which personal data for whom and for what purpose, and what instructions are applicable and who is allowed to give instructions. Any ambiguity would make it impossible for controllers or processors to fulfil their obligations under the accountability principle.
58. Where the parties providing or using certain processing services, the description (details) of the processing, the applicable technical and organizational measures, the instructions from the controller concerning the processing of personal data, the specific restrictions and/or additional safeguards concerning data of special category, the authorized sub-processors, and/or the technical and organisational measures by which the processor is required to assist the controller differ, the parties should be required to complete further Annexes I to VII, unless the differences are very limited and the exceptions clearly described in the Annexes.
59. In the case of a complex contract, which for example comprises several parties or several purposes, it must always be clear which Annex (or in case of limited deviations in one single Annex: which stipulation of such Annex) applies to which specific situation or relation. It is necessary to clearly identify and distinguish the different processing activities.

For the European Data Protection Supervisor

The European Data Protection Supervisor

(Wojciech Wiewiorowski)

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Guidelines



Guidelines 01/2023 on Article 37 Law Enforcement Directive

Version 2.1

Adopted on 19 June 2024

Version history

Version 1.0	27 September 2023	Adoption of the Guidelines for public consultation
Version 2.0	19 June 2024	Adoption of the Guidelines after public consultation
Version 2.1	30 September 2024	Minor corrections in footnotes 10 and 57

Executive summary

These guidelines provide guidance on the application of Article 37 LED, in particular on the legal standard for appropriate safeguards to be applied by competent authorities pursuant to Article 37(1)(a) and (b) LED and, accordingly, on the relevant factors for the assessment of whether such safeguards exist. These guidelines therefore include an indication as to the EDPB's expectations of Member States, as negotiating parties, when envisaging concluding or amending a legally binding instrument between the concerned Member State(s) and a third country or international organisation pursuant to Article 37(1)(a) LED.

The EDPB notes that Article 35(3) LED applies to transfers carried out under Article 37 LED. Article 37 LED should therefore be applied in light of the principle that the level of data protection applicable in the European Union must not be undermined by the transfer of personal data to another jurisdiction. The EDPB concludes that Article 37 LED requires an essentially equivalent level of data protection in the recipient third country or international organisation. However, this requirement relates to the specific data transfer or category of transfers at hand. Pursuant to Article 37 LED, essential equivalence to the protection guaranteed under the LED should be ensured for that particular case and not necessarily with regard to the entire existing legislation in the third country or international organisation.

The EDPB has already adopted Recommendations on the adequacy referential under the LED, addressing which data protection principles have to be present to ensure essential equivalence with the EU framework within the scope of the LED. The EDPB considers that the principles and safeguards outlined in these Recommendations apply in substance in the context of Article 37 LED, i.e. with regard to the specific transfer or category of transfers.

A legally binding instrument in the meaning of Article 37(1)(a) LED has to be concluded by the entity empowered to enter into obligations with respect to the safeguards provided in the instrument. The international agreement should thus have the force of law. Such legally binding instrument can be enforced by the Parties and by data subjects whose personal data processing is governed by the agreement. The legally binding instrument should contain all relevant rules to allow overcoming any shortcomings or limitations of the legislation of the third country or international organisation in terms of data protection by setting a framework of appropriate safeguards that afford an essentially equivalent level of data protection.

The EDPB considers that the use of a legally binding instrument regulating personal data transfers between the Parties should, in the absence of an adequacy decision, in principle, take precedence, over an assessment by the controller according to Article 37(1)(b) LED as it provides more legal certainty, transparency, foreseeability, stability, consistency and guarantees on the effective application of data protection safeguards.

In this context, the EDPB recalls its Statement on international agreements including transfers, adopted on 13 April 2021, inviting Member States to assess and, where necessary, review their international agreements that involve international transfers of personal data. The EDPB emphasizes that consideration should be given to the aim of bringing those agreements in line with the LED requirements for data transfers, where this is not yet the case, to ensure that the level of protection of natural persons guaranteed by the LED is not undermined when personal data is transferred outside the Union.

With respect to Article 37(1)(b) LED and in light of the above-mentioned greater guarantees offered by legally binding instruments, competent authorities may rely on such an assessment only when this

is based on a careful analysis of the relevant legal framework and practices showing that the transfers in question are subject to appropriate safeguards. In assessing the risks surrounding the transfers for the purpose of Article 37(1)(b) LED, competent authorities should examine the protection of the personal data to be transferred in view of the risks their sharing with third countries raises for the fundamental rights and freedoms of the data subjects, their legitimate interests and those of other persons concerned. Knowing in detail the circumstances surrounding the data transfers conducted or to be conducted is necessary to be able to identify these risks to the rights and freedoms of natural persons, and in particular to the right to data protection, and any safeguards that are appropriate to mitigate them.

As for any other processing operation, a competent authority must be aware of and consider in a granular manner the nature, scope, context and purposes of the transfer. More specifically, competent authorities may analyse and categorise their transfers considering characteristics relevant to assess the risks posed to fundamental rights of the data subjects such as the specific purposes of the transfer, the quantity of data transferred or the seriousness of a criminal offence.

There may be cases where appropriate safeguards already follow from the third country's international commitments, its legislation and practices. In other cases, competent authorities may need to provide, to the extent they are legally competent, for additional safeguards in light of the features of the specific transfer mentioned above, to ensure an essentially equivalent level of protection to that guaranteed under the LED and national law. The commitment of the receiving authority in the third country to respect and comply with such additional safeguards is necessary so that they are effective.

The fact that the transfer mechanisms provided in Articles 36 to 38 LED operate in cascade in general also affects the accountability obligations of the controller. The accountability obligations on the controller when relying on Article 37(1)(b) LED are enhanced pursuant to Article 37(2) and 37(3) LED because it is the controller alone who determines, based on its own assessment, whether appropriate safeguards exist. This involves higher risks of inconsistencies, less transparency, and less legal certainty for data subjects in comparison with transfers legally framed by adequacy decisions or legally binding instruments.

With regard to the obligation imposed by Article 37(2) LED and taking into account the justifying reason for adopting this provision, competent authorities should inform their data protection authorities in regular intervals about the categories of transfers that were carried out under 37(1)(b) LED. The information submitted should include the receiving competent authorities as well as the number of transfers. This would allow supervisory authorities to have a general overview and to focus their action with regard to possible 'ex post' lawfulness control on specific categories of transfers.

Table of contents

1	INTRODUCTION	6
2	ESSENTIAL ELEMENTS OF APPROPRIATE SAFEGUARDS	7
2.1	The notion of transfer	7
2.2	The notion of appropriate safeguards in the law enforcement context	8
2.3	Requirements for appropriate safeguards ensuring an essentially equivalent level of data protection within the framework of Article 37 LED.....	10
3	ARTICLE 37(1)(A) LED	12
3.1	The choice of this legal mechanism for transfers	12
3.1.1	What constitutes a legally binding instrument under Article 37(1)(a)	12
3.1.2	The advantages of having such an instrument	14
3.2	The preparatory work and negotiation	14
3.3	Contents of the legally binding instrument	16
3.3.1	General aspects	16
3.3.2	Essential elements.....	17
3.3.3	Additional tailor-made clauses	20
3.4	Interplay with concluded international agreements in this field.....	21
4	ARTICLE 37(1)(B)LED.....	22
4.1	When may Article 37(1)(b) LED be used to transfer data.....	22
4.2	How to assess all the circumstances of the transfer	22
4.2.1	Factoring the risk to data subjects into the assessment of the transfer	22
4.2.2	Categorising and assessing the transfers based on their risks to the fundamental rights and freedoms of data subjects	23
4.2.3	Determining if the existing safeguards are appropriate	27
4.3	What actions to take upon concluding on the appropriateness of the existing safeguards ..	30
4.3.1	Assuming enhanced accountability obligations by using Article 37(1)(b) LED	30
4.3.2	Including categories of transfers in record of processing activities.....	31
4.3.3	Preserving the assessments with regard to transfers, reviewing and updating them....	31
4.3.4	Cooperating with supervisory authorities	32

The European Data Protection Board

Having regard to Article 51(1)(b) of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA¹ (hereinafter “LED”)

Having regard to Article 12 and Article 22 of its Rules of Procedure,

HAS ADOPTED THE FOLLOWING GUIDELINES

1 INTRODUCTION

1. This document seeks to provide guidance as to the application of Article 37 of the LED on transfers of personal data by competent authorities of EU Member States (hereinafter “Member States”) to third country authorities or international organisations competent in the field of law enforcement. In particular, these guidelines aim to provide clarity on the legal standard for appropriate safeguards to be applied by competent authorities pursuant to Article 37(1)(a) and (b) LED and, accordingly, on the relevant factors for the assessment of whether such safeguards exist.
2. These guidelines also intend to give an indication as to the expectations of the European Data Protection Board (hereinafter “EDPB”) on the safeguards for the protection of personal data required to be put in place by a legally binding instrument pursuant to Article 37(1)(a) LED. The EDPB recommends Member States, as negotiating parties, to use these guidelines as a reference when envisaging concluding or amending such instruments.²
3. In this respect, these guidelines furthermore provide guidance to national supervisory authorities (SAs) where they are consulted or otherwise involved by Member States in the negotiation of instruments pursuant to Article 37(1)(a) LED or where they subsequently review the implementation of such instruments. These guidelines also address the role of SAs in the context of the controller’s accountability obligations according to Article 37(2) and (3) LED.
4. The EDPB notes that there is an increasing call for guidance at EU level as to the practical application of Article 37 LED across Member States. In its recent position and findings on the application of the LED, the Council has considered that guidelines for Article 37 LED would be of particular importance for Member States.³ To this end, the Council expresses that such guidance should be based on a pragmatic approach taking into account the practical needs of competent authorities.⁴ The EDPB

¹ OJ L 119, 4.5.2016, p.89.

² See also Section 3.

³ Council position and findings on the application of the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, paragraph 19, 20 (<https://data.consilium.europa.eu/doc/document/ST-13943-2021-INIT/en/pdf>).

⁴ *Ibid*, paragraph 20.

included the development of guidance for Article 37 LED in its work programme⁵ and recognizes that the ability to exchange information, including personal data, is a key element for effective international cooperation in criminal matters. The EDPB wishes to emphasize that the transfer of personal data to third countries can only be permissible within and on the basis of the applicable legal framework and while ensuring a high level of protection of personal data.⁶ In line with the tasks assigned to it in Article 51 LED, these Guidelines provide an interpretation by the EDPB of this legal framework and its binding requirements set out in the law.

2 ESSENTIAL ELEMENTS OF APPROPRIATE SAFEGUARDS

2.1 The notion of transfer

5. The transfer of personal data is a processing operation under Article 3(2) LED and, as such, is subject to any general condition the LED lays down for processing operations, in addition to those it imposes specifically on transfers.
6. Within the scope of Article 37 LED, the notion of “transfer” captures different scenarios. First, the term “transfer” under Article 37 covers direct transfers by a competent authority in the EU to authorities in a third country or to multiple third countries or to an international organisation, whether made on its own initiative or at the request of the recipient. Second, the term “transfer” also includes transfers to third countries via an intermediary, such as international organisations (e.g. Interpol). This includes, for example, making data available to third countries via international databases.
7. In addition, making available personal data to third countries by granting them direct access to national databases also qualifies as a transfer.⁷ The remote access from a third country by an official of a competent authority of a Member State, such as a liaison officer, to national databases of this Member State does however not qualify as a transfer. In such cases, a transfer occurs the moment this official discloses to or shares the data with competent authorities from third countries in the exercise of his/her official functions. Queries by a competent authority in the EU in the database of a third country or of an international organisation also constitute a transfer when personal data is provided to perform the query or when (further) processed by the third country competent authority or the international organisation, including in logs.
8. For all these different scenarios, a “transfer” always includes the process of the transmission as such. Therefore, Article 37 LED and the appropriate safeguards are also applicable to data in transit between a Member State and the third country of destination.
9. Within the framework of Article 37 LED, the notion of “transfer” is not limited to individual transfer operations, but can also refer to specific categories or sets of transfers, i.e. transfers which are defined by common characteristics such as the purpose of processing or the categories of data transferred justifying a collective assessment applicable to all such transfers. Article 37, like Articles 35 and 36 in Chapter V of the LED, use the term “transfer” in the singular form, when referring in practice to

⁵EDPB Work Programme 2021/2022, p. 5 (https://www.edpb.europa.eu/system/files/2021-03/edpb_workprogramme_2021-2022_en.pdf).

⁶ Recitals 4 and 25 LED.

⁷ See the notion of transfer in the 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, 18 November 2021, para 7.

multiple operations involving transfers from one Member State to third countries.⁸ Also, Article 38 (1) LED begins by referring to “*a transfer*” or “*a category of transfers*” and ends using “*the transfer*” in its singular form to cover both situations. Furthermore, Article 38 LED allows transfers to proceed on the basis of categories, even in the absence of appropriate safeguards pursuant to Article 37 LED, where the transfer is necessary for certain purposes. *A fortiori*, transfers based on categories would also be possible where they are covered by appropriate safeguards in the meaning of Article 37 LED.⁹ In practice, it would also be excessively burdensome to require competent authorities to conduct such comprehensive assessments on every individual transferring operation. Such a requirement would run counter to one of the LED’s objectives: to facilitate the transfer of personal data to third countries and organisations, while ensuring a high level of protection of personal data.¹⁰

2.2 The notion of appropriate safeguards in the law enforcement context

10. International cooperation in criminal matters is nowadays a key element in the fight against crime and thus for the safeguarding of the EU area of freedom, security and justice. This involves the exchange of necessary information, including the transfer of personal data – not only between Member States, but also with third countries. As noted above, the LED aims to facilitate the free flow of personal data for law enforcement purposes by competent authorities within the Union, as well as the transfer of such data to third countries and international organisations, while ensuring a high level of protection of personal data.¹¹
11. A transfer, as any other processing operation covered by the LED, must first be lawful¹² and comply with the general principles relating to the processing of personal data.¹³ In addition, transfers must comply with the specific legal framework established in Chapter V of the LED. This set of legal rules establishes a structured legal framework enabling data transfers to third countries. According to Article 35(1)(d) LED, transfers are permitted if the Commission has adopted an adequacy decision pursuant to Article 36, or, in the absence of such a decision, appropriate safeguards have been provided or exist pursuant to Article 37, or, in the absence of an adequacy decision pursuant to Article 36 and of appropriate safeguards in accordance with Article 37, derogations for specific situations apply pursuant to Article 38. Thus, these provisions operate in cascade¹⁴, meaning that Articles 37 and 38 LED presuppose that the previously established transfer mechanism is not available in the case at hand.

⁸ See for instance Article 36(1) LED which refers to a “transfer” of personal data from EU Member State to a third country in the framework of adequacy decisions. Article 38(1) LED refers indistinctively to “a transfer” or a category of transfers.

⁹ Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA also uses the term « category of transfers of personal data » (Art. 2 (u)).

¹⁰ See recitals 4 and 25 LED, and paragraph 113 of CJEU Judgement C-505/19 WS v Bundesrepublik Deutschland of 12 May 2021.

¹¹ Recitals 4 and 25 LED.

¹² Article 8 LED.

¹³ Article 4 LED.

¹⁴ By way of derogation from point (b) of Article 35(1) LED, Article 39 LED does not concern transfers of personal data between competent authorities, but establishes the rules governing data transfers directly to recipients established in third countries.

12. Taking into account that the Commission, so far, has adopted only one LED adequacy decision¹⁵ and that Article 38 LED constitutes a derogation for specific cases, competent authorities for the time being are mainly dependent on appropriate safeguards as regulated in Article 37 LED in order to transfer personal data to third countries.¹⁶
13. There are two ways to establish appropriate safeguards pursuant to Article 37(1) LED. First, appropriate safeguards may be provided in a legally binding instrument; second, the controller may carry out a self-assessment of whether appropriate safeguards for personal data exist at their destination, considering all circumstances surrounding the envisaged data transfer.
14. However, the LED offers only limited guidance to competent authorities on the application of Article 37 in practice. In particular, the LED does not set out specific formal or substantive requirements for appropriate safeguards, nor does it provide a set of mechanisms or tools for establishing appropriate safeguards or any requirement to authorise the provision of appropriate safeguards, as in Article 46 General Data Protection Regulation (hereinafter “GDPR”). Only Recital 71 indicates to some extent how Article 37 LED is to be applied.
15. This may also result from the fact that the legislator has chosen to adopt a directive in order to regulate data processing in the field of law enforcement, including international cooperation in criminal matters. As such, the LED determines binding results to be achieved, while leaving to the Member States the choice of form and methods (Article 288(3) Treaty on the Functioning of the European Union (hereinafter “TFEU”)). The LED in principle aims at a minimum harmonisation across Member States, which may provide for higher safeguards for the protection of personal data in their national laws than those foreseen in the LED.¹⁷
16. The purposes of data processing under the LED, namely 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, serve the public interest. Pursuant to Article 8 LED, data processing under the LED must always be necessary for the performance of a task carried out by a competent authority for one of those purposes and based on Union or Member State law.¹⁸ The consequences of personal data processing in the police and criminal justice context, however, can be particularly serious, for example, if the data are used as incriminating evidence or otherwise may have a discriminatory effect. When applying the LED and its transposing national legislation, competent authorities should ensure that the interference with the rights of the data subjects derived from the envisaged processing is necessary and proportionate to the objective of public interest they pursue (i.e. 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).¹⁹
17. The EDPB notes that the LED explicitly links its transfer provisions to the continued safeguarding of the right to data protection²⁰. According to Article 35(3) LED, titled “General principles for transfers of

¹⁵ Commission Implementing Decision of 28.6.2021 pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, C(2021) 4801 final.

¹⁶ As far as bilateral or multilateral agreements referred to in Article 61 LED are not available (see also Section 3.4).

¹⁷ Article 1(3) LED.

¹⁸ Recital 35 LED.

¹⁹ Article 1(1) LED.

²⁰ Article 35(3) LED.

personal data”, it shall be ensured that the level of personal data protection provided by the LED is not undermined when they are transferred outside the EU jurisdiction. For adequacy decisions it is well established that Article 36 LED, read in the light of Article 35(3) LED, requires that the level of data protection in a third country or an international organisation is essentially equivalent to the level of data protection within the European Union.²¹ The EDPB notes that Article 35(3) LED also applies to transfers carried out pursuant to Article 37 LED. In particular, Article 37 LED is not framed as an exception to the general rule laid down in Article 35(3) LED. This provision should therefore also be understood and applied in light of the principle that the level of data protection applicable in the European Union must not be undermined by the transfer of personal data to another jurisdiction. Therefore, the EDPB concludes that Article 37 LED requires an essentially equivalent level of data protection in the third country or international organisation regarding the specific transfer or category of transfers.²²

18. In this regard, it is important to recall the standard set by the Court of Justice of the European Union (hereinafter “CJEU”) for essential equivalence. As specified by the CJEU, while the level of protection in the third country or international organisation must be essentially equivalent to that guaranteed in the EU, “the means to which that third country has recourse, in this connection, for the purpose of such a level of protection may differ from those employed within the European Union”²³. Therefore, essential equivalence does not require to mirror point by point the European legislation, but to in fact ensure the core elements of that legislation, in this case the LED, read in the light of the Charter of Fundamental Rights of the European Union (hereinafter “the Charter”). This is without prejudice to higher safeguards for the protection of personal data which Member States may provide in their national legislation in accordance with Article 1(3) LED.

2.3 Requirements for appropriate safeguards ensuring an essentially equivalent level of data protection within the framework of Article 37 LED

19. The EDPB recalls that adequacy decisions adopted by the Commission formally confirm, with binding effect on Member States²⁴ including their competent data protection authorities²⁵, that the level of data protection in a third country or international organisation is essentially equivalent to the level of data protection in the European Union. Therefore, adequacy decisions should focus on the assessment of the existing legal framework of the third country or international organisation concerned as a whole, based on the assessment criteria set out in Article 36 of the LED.²⁶ The EDPB notes that Article 37 LED has a different scope. Article 37 LED regulates specific transfers or categories of transfers to authorities in a third country or to an international organisation and, accordingly, the requirement of appropriate

²¹ Recital 67 LED, EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, adopted on 2 February 2021, paragraph 8 et seq.

²² For data transfers under the GDPR, the CJEU applied the standard of essential equivalence to both adequacy decisions under Article 45 GDPR and appropriate safeguards under Article 46 GDPR (Schrems II, C-311/18). For deducing the standard of essential equivalence for adequacy decisions as well as appropriate safeguards, the CJEU referred in particular to the provision of Article 44 GDPR, according to which “all provisions in [Chapter V] must be applied to ensure that the level of protection for natural persons guaranteed by [the GDPR] is not undermined.” This general rule, as well as the notion of “appropriate safeguards”, is also found in the LED. There is no indication that - contrary to the wording - the legislator intended to impose different concepts herewith under GDPR and LED.

²³ Schrems I C-362/14, paragraph 74.

²⁴ Article 288 TFEU.

²⁵ Schrems I C-362/14, paragraph 52.

²⁶ EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, adopted on 2 February 2021, paragraph 22.

safeguards relates to a specific data transfer or category of transfers. Pursuant to Article 37 LED, essential equivalence should be ensured for that particular transfer or category of transfers and not necessarily with regard to the entire existing legislation in the third country or international organisation. Therefore, the scope of the assessment of essential equivalence under Article 37 LED does not correspond to the general and wide encompassing assessments the Commission carries out in accordance with Article 36 LED based on the criteria set out therein.²⁷

20. Recital 71 LED provides some guidance on the elements that may be taken into account when assessing whether appropriate safeguards are in place. When a competent authority considers transferring personal data under Article 37(1)(a) LED, legally binding instruments could for example be legally binding bilateral agreements concluded by Member States implemented in their legal order which could be enforced by data subjects, ensuring compliance with data protection requirements and data subject rights, including the right to obtain effective administrative or judicial redress. A competent authority wishing to make use of the possibility to transfer personal data under Article 37(1)(b) LED should be able to take into account, when assessing all the circumstances surrounding the transfer, cooperation agreements concluded between Europol or Eurojust and third countries which allow for the exchange of personal data as well as confidentiality obligations and the principle of specificity²⁸. Under their respective legal framework, Europol and Eurojust are able to transfer personal data to an authority of a third country or an international organisation on the basis of such cooperation agreements. However, the agreements under which Europol or Eurojust transfer personal data can inform but cannot replace the assessment to be carried out by the controller in the Member State pursuant to Article 37(1)(b) LED. When considering such agreements in the context of Article 37(1)(b) LED, the controller in the Member State should consider if the safeguards agreed therein apply not only to the exchange with Europol/Eurojust based on the specific agreement, but also to the transfer in question. The competent authority should also take into account that the personal data will not be used to request, hand down or execute a death penalty or any form of cruel and inhuman treatment.
21. While those conditions could, according to Recital 71 LED, be considered to be appropriate safeguards, Recital 71 LED further specifies that these conditions and safeguards are not exhaustive. That said, the EDPB considers that when a competent authority is carrying out the assessment under Article 37 LED, it should analyse not only the list of elements provided for in Recital 71 but the extent to which core data protection principles and safeguards, derived from the Charter and the LED, are provided for as enforceable in the applicable legal framework of the third country, be it in a specific data protection law or in any other source of applicable law such as criminal law or criminal procedure law, to the case at hand, offering an essentially equivalent level of protection to that guaranteed in the Member State of the transferring authority.
22. The EDPB has already adopted Recommendations on the adequacy referential under the LED, addressing which data protection principles have to be present to ensure essential equivalence with the EU framework within the scope of the LED.²⁹ The EDPB considers that the principles and safeguards outlined in these Recommendations also apply in substance in the context of Article 37 LED. However, since these Recommendations pertain to adequacy decisions pursuant to Article 36 LED and therefore, in line with the rationale of Article 36 LED, take into account all possible aspects of data protection,

²⁷ See also EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, adopted on 2 February 2021.

²⁸ See Recital 71 LED.

²⁹ EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, adopted on 2 February 2021 (https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations-recommendations-012021-adequacy-referential-under-law_en).

they are not fully operational in each and every case under Article 37 LED. In fact, and as already stated, the appropriate safeguards according to Article 37 LED need to be afforded with regard to the specific transfer or category of transfers at hand. Likewise, the standard of essential equivalence under Article 37 LED can and need to be applied solely to the processing of the data that are subject to the relevant transfer. The appropriate safeguards thus depend on the data in question and the circumstances of the processing. It is therefore neither possible nor necessary to make an abstract assessment in this regard.

23. Additionally, the EDPB recalls that Article 35(1)(a), (b), (c), (e) LED lay down requirements that apply to all provisions of Chapter V and thus also to transfers carried out under Article 37 LED. In particular, personal data may only be transferred to a controller in a third country or international organisation that is an authority competent for the purposes referred to in Article 1(1) of the LED and insofar as the transfer is necessary for such purposes.³⁰

3 ARTICLE 37(1)(A) LED

3.1 The choice of this legal mechanism for transfers

24. In the absence of an adequacy decision issued by the Commission to enable personal data to be transferred to a third country or to an international organisation, data transfers can still take place if appropriate data protection safeguards are provided in a legally binding instrument between the concerned Member State(s) and the third country or international organisation.
25. The legal requirement of Article 37(1)(a) LED means that such safeguards have to be included in the text of the legally binding instrument, in order to afford to the personal data an essentially equivalent protection when being transferred to a third country or an international organisation.
26. Therefore, the legally binding instrument has to ensure that the general principles for transfers provided by Article 35 of the LED are complied with. This includes the interplay with other provisions of the Directive (e.g. the principles applicable to data processing, lawfulness of processing and data subjects' rights), in order to ensure the level of protection of natural persons provided by the LED is not undermined.
27. Furthermore, the legally binding instrument may contain higher safeguards than contained in the LED if the national law transposing the Directive so provides pursuant Article 1(3) of the LED.

3.1.1 What constitutes a legally binding instrument under Article 37(1)(a)

28. It is important to clarify from the outset what might constitute a legally binding instrument within the context of the application of Article 37(1)(a) LED. First, it should be distinguished between the mere existence of an agreement on cooperation between Parties that entails the exchange of personal data, on the one hand and, on the other hand, the existence of an agreement that regulates the processing

³⁰ It is clear from the wording of Article 35(1)(b) LED that a competent authority under the LED, as data controller, cannot engage a third country processor in case this entails transfers to such countries, whenever the data processing is carried out for a purpose set out in Article 1(1) LED. While Recital 64 refers to processors in third countries, this reference can, in light of the explicit and unambiguous wording of Article 35(1)(b) LED, only relate to a processor acting on behalf and under the instructions of the third country competent authority receiving the data and providing for appropriate safeguards. A derogation from Article 35(1)(b) LED requires an express provision as the one foreseen in Article 39(1) LED for other recipients.

of personal data and adduces the necessary safeguards. It is not sufficient to have an agreement in place (such as a MLAT), which provides for a legal basis for the judicial cooperation on criminal matters between the Parties and the inherent data exchanges. Such an agreement does not qualify as a lawful mechanism for the international transfer of personal data under this provision of the LED³¹, unless it contains appropriate data protection safeguards.

29. The rules on personal data processing may be set up on an autonomous and specific instrument, the scope of which is to regulate transfers under the LED, or alternatively they may be inserted and become part of a more general agreement on cooperation under the scope of the LED. Either way is admissible, as long as the instrument contains the necessary safeguards to extend the protection of the data to the third country or international organisation.
30. The same rationale was already applied by the EDPB in its Guidelines 2/2020 on Articles 46(2)(a) and 46(3)(b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies. Though such guidelines do not cover transfers by competent authorities for criminal law enforcement purposes³², it is relevant to underline that they as well recognize that *any legally binding and enforceable instrument should encompass the core set of data protection principles and data subject rights*.³³
31. Secondly, the legally binding instrument may assume a bilateral or multilateral form, i.e. an agreement or a convention, between a Member State and a third country or third countries or an international organisation. This instrument may also take the shape of an EU agreement, as per Article 3(2) and 218 TFEU.
32. A mere agreement between competent authorities of the Member States and the third country³⁴ may not be enough to provide for all the appropriate safeguards required by the LED, in particular redress mechanisms and enforceable rights to data subjects as interpreted in the case-law of the CJEU. Its coverage would be limited by the legal tasks of those authorities, which by themselves are not in a position to engage in commitments beyond their responsibility.
33. It might nevertheless be allowable to conclude a legally binding agreement between competent authorities insofar as the third country applicable legislation, at least to a certain extent, already ensures an essentially equivalent level of data protection, as guaranteed in the EU, implemented in its legal order and the competent authorities have the power to commit in such an agreement to put in place the necessary additional safeguards that are not provided in the existing legal framework. In such case, the agreement may limit itself to regulate concrete aspects of the data transfers, while relying on and expressly referring to the specific provisions of the Parties' legislation to provide for the appropriate safeguards with regard to the protection of personal data, including effective and independent redress for data subjects.
34. Since, according to Article 37(1)(a) of the LED, the appropriate safeguards are to be provided in the legally binding instrument, the agreement has to contain at the very least the specific referral to the applicable legal provisions of the Parties affording for those safeguards. Furthermore, this type of

³¹ This is without prejudice that such agreements may provide a general legal basis for the transfer of the data if the conditions laid down in Article 61 of the LED are met.

³² See paragraph 4 of Guidelines 2/2020, in its version 2.0, adopted in 15 December 2020 (https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines-guidelines-2020-articles-46-2-and-46-3-b-regulation_en).

³³ *Ibid*, paragraphs 65-68.

³⁴ For instance, a Joint Investigation Team (JIT) agreement only binds the Parties on what is covered by the legal tasks of the competent authorities, i.e. related to the operational aspects of the data processing.

choice is not without risk, should the assessment of the other Party's legal framework that it relies upon falls short of guaranteeing an essentially equivalent level of protection.

35. Therefore, what matters is that the entity or body which is a Party to the legally binding instrument in the meaning of Article 37(1)(a) LED is the entity empowered to enter into obligations with respect to the safeguards provided in the instrument.
36. The international agreement should thus have the force of law. As a result, it requires foreseeability for the addressees, it applies in all its elements to the transfers in question and it establishes obligations and enforceable rights to the Parties. Such a legally binding instrument can then be enforced by the Parties and by data subjects whose personal data processing is governed by the agreement.

3.1.2 The advantages of having such an instrument

37. A legally binding instrument regulating the processing of personal data allows overcoming any shortcomings from a data protection perspective, by providing in itself the appropriate safeguards that might be lacking in the legal framework of the third country or the international organisation.
38. One of the main advantages is that such an instrument establishes a clear and structured basis for the exchange of personal data within the context of police and judicial cooperation in criminal matters with enhanced legal certainty for the national competent authorities. This will certainly increase the level of compliance by controllers while reducing their accountability obligations and potential liabilities. In addition, they would be exempted from conducting assessments on the existence of appropriate safeguards in the third countries or international organisations. On the contrary, as per Article 37(1)(b) LED, the higher the discretion granted to national competent authorities to conclude on the appropriate safeguards, the more they will be held accountable for the compliance of their transfers, in order to meet the requirements of the LED.
39. The high-level involvement of Member States in a legally binding instrument (e.g. preparation, drafting, negotiation, approval) entails a commitment, which is beneficial to promote and accelerate cooperation. A stable legal framework for exchange of information will improve the progress of investigations and proceedings in the Member States.
40. A binding agreement allows tailor-made rules not only for data protection, but also to regulate other areas of cooperation between the Parties.
41. Transparency towards individuals and closer monitoring by Governments and Parliaments is another relevant advantage of having a binding legal instrument framing the data transfers and providing the respective appropriate safeguards.

In conclusion, in the absence of an adequacy decision, though the LED presents in Article 37(1) two possible scenarios for transfers subject to appropriate safeguards, the EDPB considers that the use of a legally binding instrument regulating the personal data transfers between the Parties presents significant advantages and should, in principle, take precedence. It sets a firmer and transparent legal framework with higher legal certainty, enforceable by the Parties and the data subjects. Possible shortcomings of the legislation of the recipient third country would be compensated by adducing the necessary safeguards to ensure an equivalent level of protection.

3.2 The preparatory work and negotiation

42. The negotiation of a legally binding instrument in this context requires, as part of the preparatory work, a good overview of the relevant legal framework of the third country or international organisation. While this does not require the same in-depth evaluation of the third country as the Commission would undertake for an adequacy decision, under Article 36(2) of the LED (see Section 2.3), it should consider the relevant elements required by that provision, applied to the concrete agreement.
43. Indeed, it is necessary to have an accurate understanding of the rule of law, respect for fundamental rights, the relevant legislation and its implementation in the concerned areas (e.g. police cooperation or judicial cooperation in criminal matters), as well as relevant case law that may clarify its interpretation, redress mechanisms for data subjects whose data are transferred, including international commitments the third country or international organisation has entered into. This assessment is crucial to identify shortcomings in the legal framework of the third country or international organisation and to find a way to counterweight them by adducing the necessary safeguards in the legally binding instrument³⁵.
44. For this purpose, Member States could request the other Party, also during the negotiation, to provide the needed elements to carry out or complete this assessment. Governmental bodies experienced in international affairs (e.g. Ministries of Foreign Affairs, Justice and Interior) are usually competent to negotiate these types of agreements. They often have more resources and expertise to assess the human rights and rule of law situation in third countries than the national competent authorities that transfer personal data at the operational level.
45. If the third country already has data protection legislation, that is key-indicator for the evaluation. When considering the data protection rules possibly in force in the third country or international organisation, Member States should carefully check the scope of application of that legislation, as well as whether any relevant international legal instrument adhered to was actually effectively implemented, and how, in the third country legal order. Special attention should be paid to derogations in the law enforcement field that might render the data protection safeguards ineffective, in particular regarding data subjects' rights.
46. While preparing and negotiating the terms of the agreement, it should be ensured that the concepts are understood the same way, since likely the terminology used by the Parties in their respective legal frameworks might be different (see below 3.3.1). That is a very significant issue and requires a careful approach. The objective is not to mirror the EU legal regime, but instead to ensure that there is correspondence to the EU principles and guarantees, and ultimately the legally binding instrument contains the data protection appropriate safeguards required by the LED. This is also important in view of future interpretation and enforcement, including by supervisory authorities and courts, once the agreement will be in force.
47. The Member States negotiators should also take into account that the agreement cannot contain provisions not admissible under EU or national law, which would put at risk the lawfulness of the data processing³⁶.
48. Lastly, it should be noted that a legally binding instrument may be subject to the prior consultation of the supervisory authority.³⁷ In any case, Member States are in all circumstances encouraged to engage

³⁵ This precludes Member States from accepting, without prior analysis, standard agreements proposed by third countries, which are not open to negotiation.

³⁶ See, for instance, section 2.3.4 of these guidelines about the respect for fundamental rights, in particular in the situations described in Recital 71 LED.

³⁷ The interpretation of Article 28 LED in this context has to be further clarified.

with the national SA before the conclusion of the legally binding agreement to allow for a timely, constructive and meaningful exchange in order to verify that the appropriate safeguards are in place, in line with the requirements of Article 37(1)(a) LED. In that context, the SA should be provided with all relevant information regarding the third country or international organisations, including the respective assessments made, when available.

3.3 Contents of the legally binding instrument

3.3.1 General aspects

49. Wherever the legally binding instrument does not cover exclusively data protection issues, but governs police and/or judicial cooperation in criminal matters, the data protection clauses should be clearly identified and distinguished from other clauses dealing with other kind of information, which is not personal data.
50. The essential data protection rules should be included in the clauses of the main text while detailed provisions could be described in annexes, which are still an integral part of the agreement, to avoid overburdening the text (e.g. specific security measures, categories of data subjects or data categories, specific rules on handling the information, channels of communication, procedures in case of emergency).
51. The subject matter of the agreement should not be confused with the purpose of the data processing it entails. The objective of an agreement is usually broad, though it has to fit the scope of the LED, while the purpose of the data processing should be explicit and specific. This is of key relevance as it affects the application of rules for the further processing of data by other competent authorities in the third country, as well as it influences the outcome of the application of other data protection principles, such as data minimisation and data retention (Article 4 (1) (b), (c) and (e) of the LED).
52. Moreover, having in mind the scope of the LED, provided by its Article 2, the agreement should expressly provide that the authorities of the Parties involved in the processing of personal data within the context of that legally binding instrument are competent for the purposes set out in Article 1(1) of the LED.
53. As stressed above (paragraph 46), the agreement should contain a list of relevant definitions to ensure that the Parties have a common ground of understanding and apply data protection rules in a consistent manner. Terminology may vary from the one in the EU legal framework, as long as the concepts are recognized. In this regard, the definition of ‘personal data’ is of course essential and needs to entail the exact same meaning and broad scope as under EU law; otherwise, some data processing could be excluded from the agreement. The same applies to the concept of data processing, which needs to encompass an equivalent range of processing operations. Other definitions, such as data subject, data controller, processor, third party, data recipient, competent authority, special categories of personal data, data security/data breach, onward transfer are also relevant as a basis to build on the rules.
54. In addition, including other concepts outside the data protection field (like, ‘suspect’ or ‘criminal offence’) is very useful to shape the applicable scope of data processing. More specifically, agreeing on such notions may serve, for example, to exclude political offences qualified as ‘terrorist acts’ and to facilitate the application of the principle of dual criminality. Those concepts could be retrieved from other international instruments signed by both Parties, or taken directly from an EU legal text.

55. The text of the agreement should contain, in the text itself, all relevant data protection rules governing the data processing to be carried out in the context of such instrument. Consequently, general references to the national or international legal frameworks should not be inserted in the agreement; otherwise, that would exclude such matters from being regulated in the text of the agreement itself, where the appropriate safeguards should be provided. Such referral³⁸ should only be done, instead, to specific provisions of the legislation providing concrete safeguards, and only after a thorough assessment of the third country's legislation indicating that the level of protection ensured by the LED is not weakened. All safeguards need to be provided in the agreement in a legally binding form.
56. It should be underlined that specific conditions or restrictions on the use of data could be imposed by Member States³⁹ in the text of the agreement, following national legal requirements or specific operational needs. Indeed, Article 1(3) of the LED provides for the possibility of Member States having higher safeguards than those established in the Directive for the protection of the rights and freedoms of the data subjects.
57. In conclusion, the legally binding instrument should contain all relevant rules to allow overcoming any shortcomings or limitations of national legislation of the third country in terms of data protection by setting a framework of appropriate safeguards that afford an essentially equivalent level of data protection to the one guaranteed in the EU.

3.3.2 Essential elements

58. In order to provide the appropriate safeguards, and in view of the data protection principles referred to in Chapter 2 of these Guidelines, the legally binding instrument should contain a set of essential elements in the main text. Eventually, more detailed requirements may be introduced in an annex, which will be full part of the agreement, while avoiding overburdening the main text.
59. Against this background, in light of and without affecting the standard of essential equivalence, the following elements should in particular be addressed in the legally binding instrument⁴⁰:
- i. Determine scope as much as possible by specifying the purpose(s) of the processing and areas covered. A catalogue of offences or identification criteria based on penalties thresholds should be envisaged;
 - ii. Describe the categories of data subjects affected by the processing and the respective categories of personal data to be transferred (see paragraph 54). In case special categories of data, referred to in Article 10 of the LED, are to be processed, clearly identify which personal data will be at stake and provide that the processing may only take place where strictly necessary and subject to additional safeguards for the rights and freedoms of the data subject. The additional protective measures should be expressly described in the agreement. Exclude, however, any profiling of the data subject that would result in discrimination on the basis of the processing of special categories of data;

³⁸ The references to legislation should be specific and not general. See also paragraph 34.

³⁹ Recital 65LED states that *Member States should provide that any specific conditions concerning the transfer should be communicated to third countries or international organisations.*

⁴⁰ When a multilateral agreement is at stake involving several third countries and different levels of protection, all appropriate safeguards should be included in the text of the agreement in a comprehensive manner to ensure the highest possible minimum common denominator.

- iii. Provide that competent authorities who will be exchanging data are competent for any or all general purposes set out in Article 1(1) of the LED. The identification of the competent authorities for the Parties may be inserted in the annex or referred to further declarations by the Parties;
- iv. Provide that data should not be further processed by the identified competent authorities of the receiving Party for another purpose, without previously informing the transferring Party, duly justified, and in any case only for compatible use. The Parties should ensure that the specific purposes for which data is to be further processed are still within the scope of the LED;
- v. Exclude the disclosure to other authorities of the receiving Party, unless it has been provided in advance [set period] written information to the transferring Party, which may object to such data sharing or impose certain conditions for the processing. The information provided to the transferring Party shall identify the data recipient authority or body, which has to be an authority competent for the purposes referred to in Article 1(1) of the LED, and state the reasons for disclosing the data and the categories of data shared. Further processing of the data shall be limited to the general purposes set out in Article 1(1) of the LED. The Parties shall ensure that where data is shared to other authorities of the receiving Party the data will be processed under the same conditions as set out in the agreement and be afforded the same protection;
- vi. Provide that data processed should be relevant, adequate and limited to what is necessary for the purpose for which it was transferred and further processed;
- vii. Provide that data should be accurate and up-to-date. If any Party becomes aware that the data transferred or being processed is inaccurate or out-of-date, it shall notify the other Party without delay. Where it is confirmed that the data is inaccurate or out-of-date, each Party shall take every reasonable step to rectify or erase the data concerned;
- viii. Determine that the data transferred and further processed shall not be kept indefinitely but it shall only be retained for the period necessary to achieve the purpose for which it was transferred and further processed. Specific restrictions could be imposed on data storage periods;
- ix. Exclude automated individual decision-making, including profiling, based on the data transferred, which would produce adverse legal consequences or otherwise significantly affect the data subject, unless appropriate safeguards for the rights and freedoms of the data subject are established in the third country legal framework or in the text of the agreement. Such safeguards could include, for example, the provision of specific information to the data subject and the right to obtain human intervention on the part of the controller, to obtain an explanation of the decision reached after such assessment or to challenge the decision;
- x. Provide for the obligation of the Parties to adopt adequate and necessary security measures, of technical and organisational nature, to ensure that personal data is kept confidential and is protected against accidental or unlawful access, destruction, loss, alteration, or unauthorised disclosure. More detailed security measures could be developed in an annex (e.g. encryption of data, access controls for users based on the principle of 'need-to-know', existence of audit logs

for monitoring users' activity and so forth). It is essential that security measures should cover data processed in the place of destination, as well as in transit;

- xi. Provide that any personnel who processes personal data is bound by professional secrecy or any other statutory obligation of confidentiality, and, if applicable, that the level of confidentiality assigned to the information by the requested authority should be ensured by the requesting authority. Detailed rules may be established in the annex, for example if the Parties agree to apply the security levels used by Interpol;
- xii. Provide that, in case of a personal data breach affecting the data transferred, the concerned Party shall notify immediately the other Party and provide a description of the incident, including its immediate impact, and the relevant measures taken or proposed to be taken to address the breach and mitigate any adverse effects;
- xiii. Exclude the onward transfers to third countries or international organisations, unless prior written authorisation is obtained from the transferring Party, taking into account the requirements of Article 35(1)(e) LED. For that purpose, it should be established that the information provided to the transferring Party shall, at least, identify the country of destination or the international organisations and the data recipient, it shall state the reasons for the onward transfer, including the criminal offence involved, and the categories of data transferred. Data transferred onward should be protected by the same conditions and safeguards as in the transferring Party;
- xiv. Ensure that each Party keeps a record of all written exchanges of information required by the agreement, in particular the requests for authorisation, the authorisations given, notifications and so forth. This record is a tool for accountability and enables self-auditing and monitoring of the implementation of the agreement by SAs;
- xv. Ensure, at least, that data subjects have the right of access, rectification and erasure of the personal data concerning them. Identify to which authorities data subjects should address their requests or, at least, provide for the obligation to have that information publicly available and easily accessible at all times;
- xvi. Derogations to these rights have to be expressly established in the agreement and applied only if necessary and proportionate in a democratic society with due regard for the fundamental rights of the natural person concerned. It should be provided that the limitations to the rights are only possible, partially or fully, to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, to protect public security or national security, and to protect the rights and freedoms of others;
- xvii. Ensure independent oversight, monitoring and enforcing compliance with data protection requirements;
- xviii. Ensure administrative and judicial redress, identifying the existing mechanisms, towards which data subjects may enforce their data protection rights;

- xix. Include in the agreement a consultation and suspension clause, in case of breach of its data protection rules until the situation is resolved. Such clause should also cover situations when legislative developments undermine somehow the safeguards afforded by the legally binding instrument;
- xx. Provide that, in case of suspension or termination of the agreement, the personal data already transferred shall keep being processed under the conditions set out by the agreement.

3.3.3 Additional tailor-made clauses

60. Supplementary clauses, tailor-made for specific contexts, and providing additional safeguards, can be inserted at the discretion of the Parties and in principle regarded as best practice.

Some examples of such rules are:

- i. Provide that the Parties exchange on a regular basis information on the exercise of rights by data subjects, including statistics on the number of requests and their outcome, notably the number of cases where the right was restricted. In addition, the Parties can agree to keep a record of all requests submitted for a certain period yet to be defined;
- ii. Provide for the possibility of indirect exercise of data subject rights via an independent body, e.g. the national data protection supervisory authorities.
- iii. Provide that the Parties exchange relevant information about the use of redress mechanisms related to the application of the agreement, including the decisions taken on that account;
- iv. Include in the data subjects' rights catalogue the right to have the data processing restricted, pursuant Article 16 of the LED, while the accuracy of the personal data is still being established. During that period, the Parties should limit the use of such data, in particular the data should not be further transmitted to any third party;
- v. Provide that, in case of justified urgent need, essential for the prevention of an immediate and serious threat to public security of the Parties of this agreement or of the third State concerned, the data may be onward transferred to that third State without prior authorisation. In such a case, information shall be provided to the other Party immediately afterwards;
- vi. Set a minimum period of time for keeping the record of notifications and authorisations given within the context of the agreement, referred to in paragraph 60 (xiv) of these guidelines.
- vii. Obligation to report to the other Party if there are changes in the legal framework that might significantly affect the agreement;
- viii. Furthermore, in a situation of suspension or termination of the agreement shorter retention periods could be envisaged and a prohibition for the receiving Party to continue with any onward transfer of data;
- ix. The data of the personnel of the competent authorities exchanging the data should also be protected. As a result, such data could also be included in the list of categories of data with reference to that specific category of data subjects;

- x. Provide that a contracting Party may not invoke the fact that another Party has transferred incorrect or out-of-date data to relieve itself of its responsibility under its national law towards the data subject.

3.4 Interplay with concluded international agreements in this field

61. Article 61 LED is a transitional “grandfathering” clause, which, in the same vein as Article 60 LED⁴¹, provides that those international agreements involving the transfer of personal data to third countries or international organisations, which were concluded by Member States prior to the entry into force of the law enforcement directive, and which complied with pre-existing EU law, shall remain in force until amended, replaced or revoked.
62. The LED did not provide for a fixed deadline for their amendment to bring them into conformity with the appropriate safeguards required by the LED, and more specifically by Article 37(1)(a)LED, if these agreements do not contain already all of these safeguards. Consequently, pursuant to Article 61 LED, competent authorities from Member States may continue using these agreements to transfer data to third parties until these agreements are amended, replaced or revoked. That said, under EU law, Member States have a general obligation to bring all their international commitments in compliance with EU law. Therefore, if any existing agreement would not comply with the requirements of Article 37(1)(a) LED, it should be reviewed.
63. Furthermore, Member States must process the data received in the framework of these agreements in accordance with the LED and national law. In addition, new amendments or replacements of existing agreements, or new agreements Member States may conclude will need to contain all the necessary appropriate safeguards to comply with the LED and qualify as a “legally binding instrument” under Article 37(1)(a) LED.
64. It should be recalled that the EDPB, in its Statement 04/2021 on international agreements including transfers⁴², adopted on 13 April 2021, invites *Member States to assess and, where necessary, review their international agreements that involve international transfers of personal data*. For agreements concluded prior to 6 May 2016, this review should be done in order to determine whether, while pursuing the important public interests covered by the agreements, further alignment with current Union legislation and case law is needed.
65. The EDPB emphasizes that consideration should be given to the aim of bringing those agreements in line with the LED requirements for data transfers, where this is not yet the case, to ensure that the level of protection of natural persons guaranteed by the LED is not undermined when personal data is transferred outside the Union.

⁴¹ Nevertheless, Article 62(6) of the LED provides that the Commission shall review Union legal acts, including those referred to in Article 60, in order to align them with the LED. For that purpose, see COM(2020) 262 final, where the Commission identifies that the Prüm Decisions need to be revised in order to align, inter alia, rules on transfer of personal data to a third country or international organisation with the LED (<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0262>).

⁴² See EDPB Statement 04/2021 on international agreements including transfers, adopted on 13 April 2021, p. 1 (https://edpb.europa.eu/system/files/2021-04/edpb_statement042021_international_agreements_including_transfers_en.pdf).

4 ARTICLE 37(1)(B)LED

4.1 When may Article 37(1)(b) LED be used to transfer data

66. The mechanisms of the legal framework for transfers listed under Chapter V of the LED operate in cascade.⁴³ Consequently, competent authorities may resort to Article 37(1)(b) LED to transfer data to a third country or to an international organisation only where there is no adequacy decision issued under Article 36 LED. In the absence of an adequacy decision the use of a legally binding instrument should in principle take precedence over an assessment according to Article 37 (1)(b) LED, covering the transfer. The controller should verify this in a first step⁴⁴. While the standard of essential equivalence applies to both alternatives of Article 37(1) LED, legally binding instruments provide transfers of personal data with more legal certainty, transparency, foreseeability, stability, consistency and guarantees on the effective application of data protection safeguards, especially if the transfers are frequent, massive, structural or occur on a large-scale. The conclusion of a legally binding instrument under Article 37(1)(a) on a specific category/ies of transfers would make self-assessments under Article 37(1)(b) no longer necessary for those transfers.
67. The term “transfer” may be understood in the context of Article 37(1)(b) as encompassing specific categories or sets of transfers which are defined by some common characteristics⁴⁵ and one-time transfers to third countries or international organisations. The transfers conducted under Article 37(1)(b) LED may thus also be frequent, structural or large scale if they comply with all the requirements of the LED and the transposing national law, including those of Article 35 LED. The transfers must be covered by safeguards that are appropriate to ensure for that specific transfer or category of transfers an essentially equivalent level of protection to that guaranteed under the LED⁴⁶ and national law.⁴⁷

4.2 How to assess all the circumstances of the transfer

4.2.1 Factoring the risk to data subjects into the assessment of the transfer

68. The general objective of the LED and national transposing law is to protect the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data, while ensuring that competent authorities are able to exchange personal data where EU or national law allows it for the performance of their tasks in the public interest.⁴⁸ This objective of facilitating and strengthening data sharing, while ensuring a high level of protection of personal data, also comprises international cooperation in criminal matters.⁴⁹

⁴³ Art.35(1)(d) LED.

⁴⁴ In this regard, the controller should pay particular attention to the applicability and validity of the adequacy decision and the legally binding instrument. In addition, the EDPB encourages controllers to carefully consider planned or ongoing negotiations for a legally binding instrument under Article 37(1)(a) LED before proceeding to transfers under Article 37(1)(b) LED, in order not to undermine such negotiations.

⁴⁵ These include the purposes for which the information is processed, the categories of data subjects part of the transferred data, the criminal offence and/or its seriousness, the types and number of authorities to which data is transferred, the authority at the origin of the transfer (e.g. police, judicial), the country or countries to which data is transferred, and the nature and conditions of the execution of the criminal penalty (see Section 4.2.2 below).

⁴⁶ Art. 35(1) LED.

⁴⁷ Art. 1(3) LED.

⁴⁸ Art. 1(2) LED and Recital 35 LED.

⁴⁹ Recitals 4 and 25 LED.

69. The protection of the personal data exchanged in international cooperation is therefore an essential factor that competent authorities from the EU must take into account in their assessment of when and how to transfer data to authorities in third countries. Competent authorities should also examine the protection of these data in view of the risks its sharing with third countries raises for the fundamental rights and freedoms of the data subject on whom data is transferred, their legitimate interests and those of other persons concerned.⁵⁰ This is especially important when using Article 37(1)(b) LED to transfer data to third countries, in the absence of adequacy decisions or legally binding instrument covering a transfer.⁵¹ Competent authorities should notably assess before processing personal data, including transferring it to third countries, whether such processing is necessary and proportionate for the purpose they pursue under the LED⁵² in the light of all the circumstances of the transfer.
70. There are other factors, independent from the protection of the personal data of the data subject, which competent authorities should duly take into account before proceeding with a transfer. Some of these additional factors are the legal framework permitting the exchange of data (e.g. bilateral or multilateral agreement or instrument, reciprocity or comity), the importance of the sharing for the criminal investigation or procedure, the confidentiality level of the data, requirements from criminal procedural law, the dual criminality principle, the impact on other fundamental rights of the data subject, and possible political or diplomatic considerations.⁵³

4.2.2 Categorising and assessing the transfers based on their risks to the fundamental rights and freedoms of data subjects

71. Knowing in detail all the circumstances surrounding the specific data transfers conducted or to be conducted is necessary to be able to identify the risks to the rights and freedoms of natural persons, and in particular to the right to data protection, and any safeguards that are appropriate to mitigate them.⁵⁴
72. As for any other processing operation, a competent authority must be aware of and consider in a granular manner the nature, scope, context and purposes of the transfer.⁵⁵ More specifically, competent authorities should analyze and categorise their transfers considering the characteristics mentioned below. These characteristics are relevant to assess the risks posed to fundamental rights of the data subjects by each transfer in their relevant context.
73. **Categories of data subjects:** the LED⁵⁶ and other EU⁵⁷ and international legal frameworks⁵⁸ require distinguishing between different categories of data subjects (e.g. suspects, convicted criminals, victims, witnesses, persons of interest, associates, missing persons). The risks to the rights of data subjects will vary depending on the category of the subject and the context in which the transfer is

⁵⁰ Recitals 28, 37, 50, 51, 52, 58, 60, Articles 19, 27 LED.

⁵¹ See for example the additional risks to data subjects where data is transferred abroad on their ability to exercise these rights which recital 74 LED notes. The absence of adequacy decisions or legally binding instrument increases these risks.

⁵² See references to the application at the operational level of the necessity and proportionality principle in Recitals 26, 29, Art.4(2)(b) LED.

⁵³ Another exception for the transfer may concern the national security of the Member State or the third countries. Competent authorities should assess in accordance with their national law, whether the assistance provided could threaten the sovereignty, security, public order or other essential interests of the State.

⁵⁴ Article 37(1)(b), Recital 71 LED.

⁵⁵ See the responsibilities of the controller for any processing of data in Recitals 50, 51, 58, and Article 19 LED.

⁵⁶ Recital 31 and Art. 6 LED.

⁵⁷ Recital 43, Art.18 (3)(a) and Art. 18 (5), Art.30, 34(2)(a), Annex II Europol Regulation.

⁵⁸ Article 44 INTERPOL's Rules on the Processing of Data.

made. This will be especially the case where the competent authority transfers special categories of personal data, as defined in Article 10 LED.

Example: The transmission of an image of a victim of child sexual exploitation to competent authorities in third countries to identify the victim will require enhanced data security confidentiality safeguards, and data minimisation to avoid the re-victimisation of the victim of sexual exploitation. Some of these safeguards could be restricting the access to these data to analysts and investigators from services specialised and trained in the area of online child sexual exploitation; foreseeing technical measures to ensure the separation of these data from other police data and databases; and minimising the amount of information transferred (e.g. full image, sanitised image, or hash code of the image) depending on its categorisation and the specific purposes sought through the cooperation. These safeguards could thus be different from those applicable to an international request for location and arrest of a convicted criminal, which may be widely shared among law enforcement authorities (and even the public in some cases), and include as much information as possible to identify and find the individual.

74. **Specific purposes of the transfer:** a transfer must serve one of the purposes described under Article 1(1) LED, namely, 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. Within these general purposes, transfers serve specific purposes such as to locate and obtain information on a person in the framework of a criminal investigation, to identify a person or to carry out crime analysis to identify threats, trends and criminal networks. To ascertain the safeguards that are appropriate for this transfer, the competent authority should determine as much as possible which of these specific purposes the transfer is pursuing. The choice of adequate measures to protect the rights of data subjects may also depend on whether a Member State competent authority is transferring data to obtain more data for its own purposes, such as for a criminal investigation it is conducting; or whether this competent authority is responding to a request made by a foreign authority for its own criminal investigation and prosecution.

Example: Finding a missing person in the framework of a criminal investigation may in practice require the transfer of more personal information and the disclosure of these data to multiple authorities in third countries (and possibly also to the public) than locating a witness of a serious crime. In the latter case, the protection of the witness and his/her rights may warrant more stringent (confidentiality) measures, as the personal information may be considered particularly sensitive in this context. The purpose of finding a missing person, on the one hand, and a witness to a serious crime, on the other, may thus necessitate different data protection safeguards.

Example: Transferring data on known movements across borders of foreign terrorist fighters to conduct strategic crime analysis together with a third country authority⁵⁹ to help prevent crime may require different safeguards than providing data to a third country's authorities to help it detect and prosecute a suspect for a serious crime.⁶⁰ In the first case, the purpose pursued to produce strategic crime analysis reports to inform law enforcement strategies to tackle international terrorism may justify setting longer retention periods and more flexible standards of accuracy and reliability for the data processed, as well as limiting the access to data to a specialised body (e.g. police intelligence information units) in the receiving country. In the second case, the retention periods will usually need to be shorter and the data of high quality and accuracy to prevent prejudicing persons other than the

⁵⁹ See for example Art18 (2)(b) of the Europol Regulation and Article 10(2)(h) of INTERPOL's Rules on the Processing of Data.

⁶⁰ See for example Article 10(2)(a) of INTERPOL's Rules on the Processing of Data.

suspect due to misidentifications or applying coercive measures on the suspect that may no longer be necessary and are based on outdated information, while the data may need to be widely shared among law enforcement authorities (and in some cases the public) to find the suspect.

75. **Quantity and nature of data transferred:** The risks to the rights of data subjects will vary depending on the quantity of data transferred, as well as on its nature (e.g. sensitive data). The different stages and purposes of an investigation, in compliance with the data minimisation principle, may lead to transfers which may vary in the amount and categories of data.

Example: If a police service is seeking to identify a person whom it has very little information about in the beginning of an investigation, the transfer request would initially likely be limited to the question of whether the data subject is known to the police services of one or more third countries. The answer provided by the third country would allow the police and justice either to direct the investigation to another country or to start a more extensive data exchange. In the same vein, the type of investigation may also require the exchange of a single piece of data.

76. **Types and number of authorities to which data is transferred:** Article 35(1)(b) LED provides as a condition for transfers that the authority in the third country or international organisation is competent for the purposes referred to in Article 1(1) LED. The specific purpose for which a transfer or category of transfers is conducted should determine to which specific authorities in the third country data may be transferred to guarantee that data is processed in the third country only for the purposes for which it has been transferred (principle of specificity).⁶¹ The legal framework of the third country or the additional safeguards provided in the data exchange should establish the principle of purpose limitation and prevent it from being processed for incompatible purposes. Entities in the third country may have a mandate to serve different purposes (e.g. crime prevention, national security, etc.), which may require to define more granularly the service within that entity accessing the data. The wider the dissemination of data in the third country among its authorities, the higher the data protection risks to the fundamental rights, such as its use for purposes incompatible⁶² with those for which it was provided and data breaches. These risks thus need to be factored into the assessment of whether to transfer data to certain third countries and with which safeguards.

Example: A competent authority in a Member State may transfer data only to units in the third country's police forces dedicated to information on organised crime for the purpose of conducting joint crime analysis. The competent authority may request that such information is not shared with other authorities within those countries that are not directly competent in this area, in order to limit data protection risks and undermining its criminal investigation. The competent authority may also ensure that the receiving authorities in the third country commit themselves to informing the competent authority before any further processing of these data by different units or police services for different purposes, so that the competent authority may signal its objection to this processing if it so wishes.

77. **Seriousness of the criminal offence:** the seriousness of the criminal offence⁶³ is also relevant to evaluate the risks that the transfer may pose to the rights of a data subject, and which safeguards would be appropriate to mitigate such risks.

⁶¹ Recital 71 LED.

⁶² Article 4(1)(b) and Recital 29 LED.

⁶³ Recital 65, Art. 35(1)(e) LED.

Criminal offences with low penalties foreseen may not justify neither sending the data as part of requests to third countries, nor to respond to requests on such types of offences received from authorities in third countries.

The dual criminality principle often present in MLATs would also be relevant in this regard to determine if data may be shared with third countries.

Advancing criminal investigations in cases of serious crimes such as terrorism and organised crime may justify sending out personal data as part of a request. At the same time, in order to avoid the risk of contributing to political prosecutions or the application of death penalty or any form of cruel and unusual punishment,⁶⁴ the seriousness of the criminal offence would also warrant a reconsideration of the transfer or adopting additional safeguards when responding to a request in this area from certain countries.

Example: In light of the risks to the rights and freedoms of the data subject once the data will be transferred in a third country, the competent authority of an EU country may consider it disproportionate to send a request for international police cooperation on a criminal offence with a penalty of less than a year of prison, or to respond to a request for information on a person wanted for the offence of bounced cheques. Conversely, it may deem necessary and proportionate to send personal data to an authority of a third country as part of request in a case of terrorism. In this case, the competent authority would still have to subject the transfer of personal data to appropriate safeguards to mitigate any potential and unwarranted risks to the rights of the data subject.

78. **Authority at the origin of the transfer:** the authority at the origin of the transfer may be judicial, police, other law-enforcement authorities or other bodies or entities entrusted by Member State law to exercise public authority and public powers for the purpose of the LED.⁶⁵ The nature of this authority, its institutional mandate and independence, and the rules to which it is consequently subject, may also be relevant in the assessment of the risks of the transfer and the safeguards it may need in accordance with those provided for example in national rules on judicial proceedings.⁶⁶

Example: Personal data that is sent to third countries on the request or with the authorisation of a judicial or other independent authority of a Member State provides additional guarantees and safeguards to the rights and freedoms of a data subject than when a competent authority such as a police body shares personal data informally with its counterpart in a third country.

79. **Country or countries to which data is transferred:** the overall level of protection of personal data⁶⁷ and other fundamental rights and freedoms in the third country is another important feature of the transfer. The level of protection of natural persons provided for in the EU by the LED cannot be undermined by the transfer to third countries or international organisations.⁶⁸ The competent authority should take into account elements in the third country such as those listed under Article 36(2) LED together with the others mentioned above before deciding on transferring the data and on the safeguards that would be appropriate to ensure an essentially equivalent level of protection of the data in the light of the risks involved, including rules for onward transfers.

⁶⁴ Recital 71 LED.

⁶⁵ Recital 11 and Art. 7 LED.

⁶⁶ Recital 49 LED.

⁶⁷ Recital 65 LED.

⁶⁸ Recital 64, Art. 35(3) LED.

Example: Sharing data with a third country on which there are doubts over its general respect for the rule of law, human rights, and fundamental freedoms entails higher risks to the rights and freedoms of a data subject, including the right to data protection.

80. **Nature and conditions of the execution of the criminal penalty in the third country:** The risks to the rights and freedoms of the data subject will be higher where there is a possibility that, based on the personal data transferred, the data subject faces death penalty or any form of cruel and inhuman treatment in the third country (see also paragraph 78 above).⁶⁹ The competent authority should then assess whether to proceed with the transfer and any safeguards to be added to prevent this risk.

Example: A competent authority receives a request from a third country for information that could serve to sentence the data subject for a drug trafficking offence, which some third countries punish with the death penalty. The competent authority makes such data transfers contingent on obtaining a commitment of the third country not to impose death penalty or any form of cruel and inhuman treatment.

4.2.3 Determining if the existing safeguards are appropriate

81. Article 37(1)(b) would operate in cases where there would be no adequacy decision (Article 36 LED) or legally binding instrument (Article 37(1)(a) LED) between the EU Member State and the third country providing appropriate safeguards for categories of transfer. There may be cases where appropriate safeguards already follow from the third country's international commitments, its legislation and practices. In other cases, competent authorities may need to provide, to the extent they are legally competent, for additional safeguards in light of the features of the specific transfer mentioned above, to ensure an essentially equivalent level of protection to that guaranteed under the LED and national law, for example, depending on the individual case, via MoUs, exchange of letters or other kind of arrangements (see also paragraph 86).

International instruments and frameworks to which the third country is bound

82. The third country and its authorities may already have committed themselves to privacy and data protection obligations and standards via multilateral or bilateral international instruments and frameworks binding also Member States and their authorities. Without prejudice to the possible application of the transitional provision of Article 61 LED to them⁷⁰, the ratification of such instruments may not by itself provide for an essentially equivalent level of protection, as this will depend, in particular, on their specific implementation in each country (e.g. ratification of Convention 108 and additional protocols).⁷¹ Yet, the ratification of such international instruments may still be relevant as a factor in the assessment of existing safeguards⁷² and the level of protection under Article 37(1)(b) LED.
83. The competent authority may share or send the data to one or several third countries via an intermediary such as an international organisation (e.g. Interpol). These international bodies may already have legal frameworks for transfers that may protect the data transferred with some appropriate safeguards.⁷³ The competent authority will be able to rely on these safeguards and may,

⁶⁹ Recital 71 LED.

⁷⁰ See Section 3.4 above.

⁷¹ The EDPB does not assess in these Guidelines the extent to which specific existing instruments meet the requirements of Article 37(1)(a) LED.

⁷² See paragraph 46.

⁷³ All Member States are INTERPOL Members. When processing data in or from the INTERPOL Information System Member States and third countries members to this international organisation must apply INTERPOL's Constitution, its Rules on the Processing of Data (RPD), and other secondary law of this organisation and specific

in light of all the circumstances of the transfer, need to complement them with additional safeguards in order to meet the standard of an essentially equivalent level of protection with the LED and national law. These frameworks usually allow for the imposition of additional conditions or safeguards to the data transferred (e.g. no use of the data in judicial proceedings, limitation to specific purposes, data access restrictions, shorter retention periods for data, onward transfers etc).

Legislation and practices of the third country

84. A third country's legislation and the practice of its authorities may already provide some of the appropriate safeguards needed to ensure that the data transferred benefits from a level of protection essentially equivalent to that guaranteed under the LED and EU law, when processed in the third country. Article 36(2)(a) and (b) of the LED list some of the elements that may indicate or confirm the existence of appropriate safeguards in the third country.⁷⁴ The competent authority will still need to assess to what extent these safeguards may apply to the data transferred⁷⁵ and would be sufficient to meet the standard of essential equivalence, in light of all the circumstances of the transfer, and foresee additional safeguards to this end where needed.
85. The competent authority will need to monitor relevant developments in the third country and/or practice of its authorities and that may indicate that appropriate safeguards are not effectively applied. Appropriate safeguards must be applied in practice and not only formally. The competent authority should reassess transfers regularly and, on that basis, decide accordingly to provide additional safeguards or suspend the transfer.

Possible additional safeguards

86. To ensure that the data transferred is subject to an essentially equivalent level of protection to that guaranteed under EU or national law while it is processed in a third country or international organisation, the competent authority may add safeguards to those that may already exist. The competent authority should ensure that such additional safeguards are appropriately communicated to the receiving authority. The commitment of the receiving authority in the third country to respect and comply with these safeguards is necessary so that they are effective. International frameworks and commitments often contain provisions allowing their Parties or Members to impose additional safeguards in certain cases on the data they transfer.⁷⁶
87. Some of the possible additional safeguards are the following:

provisions governing its databases, communications infrastructure and other services (Arts. 4 and 5 RPD). Member States will need to assess if in light all the circumstances of the transfer/category of transfers these safeguards need to be complemented with additional ones to ensure that the data meets the standard of essentially equivalent level of protection when processed in the third country/ies to which it was transferred via INTERPOL. (See Recital 25 LED).

⁷⁴ See also Chapter 2 and the EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, adopted on 2 February 2021.

⁷⁵ For example, in some third countries, under their legislation and practices, some of these safeguards may only apply to nationals of that country and/or to specific categories of data or purposes of the processing.

⁷⁶ See for example the possibility under INTERPOL's Rules on the Processing of Data for Members to establish general or data-specific access restrictions to the data on other Interpol members (Articles 58 and 107-109 RPD), special conditions for use on the data transferred (Articles 45 and 66 RPD), specific data processing purposes (Article 10(3)-(5) RPD) and shorter retention periods on the data recorded in INTERPOL's databases (Article 46(4)(a) RPD). Other possibilities may include, depending on the individual case, MoUs, exchange of letters or informal arrangements, etc.

- Restricting access to the data transferred at the level of the country, authority or data;⁷⁷
- Restriction on the processing of the data to a specific purpose defined in the transfer (principle of specificity);⁷⁸
- Establishing notification and authorisation mechanisms to the competent foreign authority from which the data originates for transfers among authorities within a country;
- Defining specific conditions for the processing or handling of the data;⁷⁹
- Establishing specific data retention periods and mechanisms of automated deletion to ensure that the data is processed for the purposes for which it is provided and the validity of this purpose and the accuracy of the data is regularly checked;
- Setting out review processes and notification procedures between authorities to ensure that data remains accurate and up to date having regard to the purposes for which they are processed, and where necessary erased or rectified without delay;⁸⁰
- Establishing specific data security safeguards through technical (e.g. agreed standards, logs, encryption, authentication mechanisms) and organisational measures (e.g. designation of data security officer or department, audits, internal and external oversight, disciplinary measures) to ensure its protection against unauthorised access or unlawful processing and against accidental loss, destruction or damage;⁸¹
- Providing for consultation and joint audit and review mechanisms of the processing of data and transparency measures such as access to logs of processing of transferred data by third country;
- Demanding commitments on the non-application of death penalty or any form of cruel and inhuman treatment.⁸²

Sources of information:

88. To obtain information on the safeguards that may already exist for a transfer to a third country and ascertain if additional ones are needed, competent authorities may use sources such as the following:
- Existing EU adequacy decisions under the GDPR covering that country or one of its regions/sectors;
 - Reports on third countries produced by the Commission (e.g. Progress Reports on candidate and potential candidates to the EU);

⁷⁷ See Recital 71 LED.

⁷⁸ *Ibid.*

⁷⁹ E.g. through the use of special handling codes providing for example that data may only be used for the purpose of preventing and combating specific criminal offences; that it may not be disclosed or used in judicial proceedings without the permission of the EU competent authority; that it may not be disseminated to other authorities in the third country without the permission of the EU competent authority; and others.

⁸⁰ Article 4(1)(d) LED.

⁸¹ Article 4(1)(f) LED.

⁸² Recital 71 LED.

- Case-law of the CJEU, the European Court of Human Rights and decisions of Member States' Courts and data protection supervisory authorities in relation to transfers to specific third countries;⁸³
- Assessments already conducted by EU bodies or agencies (e.g. Europol, Eurojust, EPPO, Frontex) before concluding cooperation agreements with third countries.
- Reports or assessments produced by national Ministries of Foreign Affairs, Justice and Interior;
- Relevant legislation and case-law of that third country (including case-law of international human rights courts with jurisdiction over the third country), and decisions taken by independent administrative authorities competent on privacy and data protection matters;
- Reports of independent oversight or parliamentary bodies in that third country;
- Resolutions, reports and notifications from intergovernmental organisations on the third country on relevant aspects to data protection such as rule of law, human rights, and compliance with international rules on the processing of police data;
- Reports from other sources such as academia, civil society organisations (e.g. NGOs), etc.

[4.3 What actions to take upon concluding on the appropriateness of the existing safeguards](#)

[4.3.1 Assuming enhanced accountability obligations by using Article 37\(1\)\(b\) LED](#)

89. The fact that the transfer mechanisms provided in Articles 36-38 LED operate in cascade in general also affects the accountability obligations of the controller. In other words, the place in which the transfer mechanism is positioned in the order provided by LED is in general inversely proportional to the accountability obligations of the controller. For instance, for transfers based on adequacy decisions issued by the Commission, the controllers being bound by them should only monitor that the adequacy decision remains valid. For transfers based on appropriate safeguards under Article 37(1)(b) LED, the competent authorities should assess and, in the case of categories of transfers, regularly monitor, the appropriateness of the safeguards, which have to meet the standard of essential equivalence, and further document the details of the assessment and of the transfer.
90. This is reflected in Article 37(2) and 37(3) LED which indeed provide that the controllers have the obligation (i) to inform the supervisory authorities of categories of transfers taking place under the controller's assessment (Article 37(1)(b)); (ii) to document in detail such transfers, including as regards the assessment undertaken prior to the transfer and (iii) to make the documentation available to the supervisory authority on request. The documentation requirements are extensive and include all the elements provided for the documentation of transfers carried out under the regime of derogations, i.e. including the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and the personal data transferred.
91. The accountability obligations on the controller are enhanced because it is the controller alone who determines, based on its own assessment, whether appropriate safeguards exist. This involves higher risks of inconsistencies with other assessments of transfers, less transparency, and less legal certainty

⁸³ Some of these decisions may be found in the EDPB's registry of decisions taken under the one-stop-shop mechanism: https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_en. References to national decisions may be found in the national news section of the EDPB's website: https://edpb.europa.eu/news/news_en?news_type=2.

for data subjects in comparison with transfers legally framed by adequacy decisions or legally binding instruments. Therefore, transfers under 37(1)(b) LED should be documented in detail, including with regard to the initial assessment of the safeguards in place, while the supervisory authorities should be informed on the categories of such transfers in order to allow for an effective scrutiny.

92. With regard to the obligation imposed by Article 37(2) LED and taking into account the justifying reason for adopting this provision, the competent authorities should inform their data protection authorities in regular intervals about the categories of transfers that were carried out under 37(1)(b) LED. The information submitted should include the receiving competent authorities as well as the number of transfers per category. This would allow the supervisory authorities to have a general overview and to focus their action with regard to possible ‘ex post’ lawfulness control on specific categories of transfers.

4.3.2 Including categories of transfers in record of processing activities

93. In line with the provision of Article 24 LED the controller is under the obligation to maintain a record of all categories of processing activities under their responsibility, which shall contain the specific and detailed information provided in this provision. The duty of controllers to keep records on processing operations is one of the means to reinforce accountability. Knowing which data are processed about what kind of data subjects and for what purposes is a prerequisite for being able to be held accountable and the controller must be able to give account to the supervisory authority about the categories of data and data subjects and the purposes of its processing operations.
94. A further item to be documented under Article 24(1)(f) LED is the categories of transfers of data to ‘a third country or an international organisation’. In such cases, the third country, or international organisation respectively, must be named in the records, but evidently not the identity of the recipient, as the provision does not add anything to point c) for cases of international data transfers. Hence, reference to the categories of recipients would be sufficient.
95. The wording of Article 24(1)(f) LED implies that there is no obligation to name the means by which the controller intends to ensure an adequate level of protection in case transfers of personal data are carried out. However, interpreted in conjunction with Article 37(2) LED which pertains to specific categories or sets of transfers which are defined by some common characteristics as well as to one-time transfers to third countries or international organisations, it would be optimal if the envisaged transfer mechanism is referred in the record. In this way, the obligation of the controller to inform the supervisory authority on the categories of transfers taking place under the controller’s assessment of the existence of appropriate safeguards will be facilitated.
96. The information with regard to transfers included in the records should be kept up to date.

4.3.3 Preserving the assessments with regard to transfers, reviewing and updating them

97. One of the accountability obligations imposed on the controller in case Article 37(1)(b) applies is the detailed documentation of the transfer in line with Article 37(3) LED which should as minimum include the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and the personal data transferred. Some of these documentation requirements, e.g. the date and time of the transfer, could be fulfilled by preserving logs as prescribed by Article 25 LED according to which the competent authority should, among other things, keep logs for the disclosure of personal data including transfers.
98. Taking into account that the obligation to document the transfers is set by the legislator in order to facilitate the ‘ex post’ lawfulness control by the supervisory authorities, the documentation should

include information that is sufficient and facilitates this control. To this end, the justification of the transfer refers to the assessment of the circumstances of the transfer that takes into account all the factors analysed above for defining the transfer categories (under Section 4.2.2) and for assessing whether appropriate safeguards are in place (under Section 4.2.3).

99. In more detail the documentation of the assessment of the circumstances should include:
 - i. A statement confirming that an adequacy decision or a legally binding agreement providing appropriate safeguards were not available.
 - ii. The definition of the categories / set of transfers or specific transfer which are/is subject to the assessment.
 - iii. The identification of the risks entailed to the rights of the data subjects by the categories / set of transfers or specific transfer. In identifying the risks the following factors should be, inter alia, taken into account: the country or countries to which the data is transferred; the categories of data subjects affected (suspects, convicted criminals, victims, witnesses, persons of interest, associates); the categories (in particular whether special categories are included) and the quantity of the data transferred; the specific purpose of the transfer; the competent authorities to which the data is transferred; the seriousness of the criminal offence in relation to which the transfer of data takes place; the authority at the origin of the transfer (judicial or law enforcement authority); the nature and conditions of execution of the criminal penalty provided in the third country for the criminal offence in relation to which the transfer of data takes place; the possible existence of the death penalty in relation to the criminal offence for which the data is transferred.
 - iv. The assessment on whether appropriate safeguards with regard to the risks identified (see point iii) offering an essentially equivalent level of protection are in place. Such assessment must be based on the relevant legal framework (international commitments and domestic legislation, be it a specific data protection law or any other source of applicable law such as criminal law or criminal procedure law) and practices in the country or countries to which the data is transferred.
 - v. The registration of the outcome of the assessment. In case it is negative, assess whether additional safeguards can be provided for in MOUs, exchanges of letters and other arrangements.
 - vi. In the latter case, any additional safeguards provided for in MOUs, exchanges of letters and other arrangements.
 100. The controllers under the principle of accountability are obliged to monitor carefully if there have been or there will be any developments with regard to the factors taken into account for assessing the appropriateness of the existing safeguards that may affect the outcome of their assessment.
- #### 4.3.4 Cooperating with supervisory authorities
101. The LED integrates accountability as a fundamental data protection principle in the context of law enforcement (Article 4(4) LED). The controllers are not only responsible but they shall also demonstrate to the supervisory authorities compliance with the data protection principles provided in Article 4. To that end Article 26 LED establishes a legal obligation for controllers to cooperate with the supervisory authority when exercising its tasks. Such cooperation must be provided on request of the supervisory authority.

102. As regards the means of fulfilling this obligation, Article 24(3), 25(3) and 37(2) and (3) LED provide that the controllers should inform their supervisory authorities on categories of transfers carried out under 37(1)(b) and make available to them at their request the records of processing operations, their logs as well as the documentation required in cases where the controller has assessed the circumstances surrounding a transfer and concluded that appropriate safeguards are in place. However, there is nothing in the wording of the relevant provisions and in particular of Article 26 LED that limits the ways of cooperation. To the contrary the obligation to cooperate should be fulfilled as requested by the supervisory authority, which may include providing additional information (even originating from the destination country) and documentation, granting access to processing facilities, and explaining processing operations.
103. Violations of the obligation to cooperate with the supervisory authority could be sanctioned. In the context of the LED, the rules on penalties applicable to infringements of the provisions adopted pursuant to the LED are defined by the Member States and shall be effective, proportionate and dissuasive (Article 57 LED). Hence, infringement by a competent authority of the obligation to cooperate with its supervisory authority could lead to penalties, defined under national law, independently of the existence of other infringements of the provisions transposing the LED (such as the provisions with regard to transfers). The above considerations are without prejudice to the fact that the controllers are at every time under the obligation to implement binding decisions of their supervisory authorities exercising their corrective powers (e.g. heeding the warning with regard to a possible infringement of the data protection legal framework in case a specific transfer takes place or stop a set of transfers in case a ban is issued).