

# Guidelines



## **Guidelines 3/2019 on processing of personal data through video devices**

**Version 2.0**

**Adopted on 29 January 2020**

## Version history

Version 2.1	26 February 2020	Amending material mistake
Version 2.0	29 January 2020	Adoption of the Guidelines after public consultation
Version 1.0	10 July 2019	Adoption of the Guidelines for public consultation

## Table of contents

1	Introduction .....	5
2	Scope of application.....	7
2.1	Personal Data .....	7
2.2	Application of the Law Enforcement Directive, LED (EU2016/680) .....	7
2.3	Household exemption.....	7
3	Lawfulness of processing .....	9
3.1	Legitimate interest, Article 6 (1) (f).....	9
3.1.1	Existence of legitimate interests.....	9
3.1.2	Necessity of processing.....	10
3.1.3	Balancing of interests.....	11
3.2	Necessity to perform a task carried out in the public interest or in the exercise of official authority vested in the controller, Article 6 (1) (e) .....	13
3.3	Consent, Article 6 (1) (a) .....	14
4	Disclosure of video footage to third parties .....	15
4.1	Disclosure of video footage to third parties in general .....	15
4.2	Disclosure of video footage to law enforcement agencies.....	15
5	Processing of special categories of data .....	17
5.1	General considerations when processing biometric data .....	18
5.2	Suggested measures to minimize the risks when processing biometric data .....	21
6	Rights of the data subject .....	22
6.1	Right to access.....	22
6.2	Right to erasure and right to object.....	23
6.2.1	Right to erasure (Right to be forgotten) .....	23
6.2.2	Right to object.....	24
7	Transparency and information obligations.....	26
7.1	First layer information (warning sign).....	26
7.1.1	Positioning of the warning sign.....	26
7.1.2	Content of the first layer.....	26
7.2	Second layer information.....	27
8	Storage periods and obligation to erasure .....	28
9	Technical and organisational measures.....	28
9.1	Overview of video surveillance system.....	29
9.2	Data protection by design and by default .....	30
9.3	Concrete examples of relevant measures .....	30

9.3.1	Organisational measures .....	31
9.3.2	Technical measures.....	31
10	Data protection impact assessment .....	33

# The European Data Protection Board

Having regard to Article 70 (1e) 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<sup>1</sup>,

Having regard to Article 12 and Article 22 of its Rules of Procedure,

## HAS ADOPTED THE FOLLOWING GUIDELINES

### 1 INTRODUCTION

1. The intensive use of video devices has an impact on citizen's behaviour. Significant implementation of such tools in many spheres of the individuals' life will put an additional pressure on the individual to prevent the detection of what might be perceived as anomalies. De facto, these technologies may limit the possibilities of anonymous movement and anonymous use of services and generally limit the possibility of remaining unnoticed. Data protection implications are massive.
2. While individuals might be comfortable with video surveillance set up for a certain security purpose for example, guarantees must be taken to avoid any misuse for totally different and – to the data subject – unexpected purposes (e.g. marketing purpose, employee performance monitoring etc.). In addition, many tools are now implemented to exploit the images captured and turn traditional cameras into smart cameras. The amount of data generated by the video, combined with these tools and techniques increase the risks of secondary use (whether related or not to the purpose originally assigned to the system) or even the risks of misuse. The general principles in GDPR (Article 5), should always be carefully considered when dealing with video surveillance.
3. Video surveillance systems in many ways change the way professionals from the private and public sector interact in private or public places for the purpose of enhancing security, obtaining audience analysis, delivering personalized advertising, etc. Video surveillance has become high performing through the growing implementation of intelligent video analysis. These techniques can be more intrusive (e.g. complex biometric technologies) or less intrusive (e.g. simple counting algorithms). Remaining anonymous and preserving one's privacy is in general increasingly difficult. The data protection issues raised in each situation may differ, so will the legal analysis when using one or the other of these technologies.
4. In addition to privacy issues, there are also risks related to possible malfunctions of these devices and the biases they may induce. Researchers report that software used for facial identification, recognition, or analysis performs differently based on the age, gender, and ethnicity of the person it's identifying.

---

<sup>1</sup> References to "Member States" made throughout this opinion should be understood as references to "EEA Member States".

Algorithms would perform based on different demographics, thus, bias in facial recognition threatens to reinforce the prejudices of society. That is why, data controllers must also ensure that biometric data processing deriving from video surveillance be subject to regular assessment of its relevance and sufficiency of guarantees provided.

5. Video surveillance is not by default a necessity when there are other means to achieve the underlying purpose. Otherwise we risk a change in cultural norms leading to the acceptance of lack of privacy as the general outset.
6. These guidelines aim at giving guidance on how to apply the GDPR in relation to processing personal data through video devices. The examples are not exhaustive, the general reasoning can be applied to all potential areas of use.

## 2 SCOPE OF APPLICATION<sup>2</sup>

### 2.1 Personal Data

7. Systematic automated monitoring of a specific space by optical or audio-visual means, mostly for property protection purposes, or to protect individual's life and health, has become a significant phenomenon of our days. This activity brings about collection and retention of pictorial or audio-visual information on all persons entering the monitored space that are identifiable on basis of their looks or other specific elements. Identity of these persons may be established on grounds of these details. It also enables further processing of personal data as to the persons' presence and behaviour in the given space. The potential risk of misuse of these data grows in relation to the dimension of the monitored space as well as to the number of persons frequenting the space. This fact is reflected by the General Data Protection Regulation in the Article 35 (3) (c) which requires the carrying out of a data protection impact assessment in case of a systematic monitoring of a publicly accessible area on a large scale, as well as in Article 37 (1) (b) which requires processors to designate a data protection officer, if the processing operation by its nature entails regular and systematic monitoring of data subjects.
8. However, the Regulation does not apply to processing of data that has no reference to a person, e.g. if an individual cannot be identified, directly or indirectly.

Example: The GDPR is not applicable for fake cameras (i.e. any camera that is not functioning as a camera and thereby is not processing any personal data). *However, in some Member States it might be subject to other legislation.*

Example: Recordings from a high altitude only fall under the scope of the GDPR if under the circumstances the data processed can be related to a specific person.

Example: A video camera is integrated in a car for providing parking assistance. If the camera is constructed or adjusted in such a way that it does not collect any information relating to a natural person (such as licence plates or information which could identify passers-by) the GDPR does not apply.

- 9.
10. Notably processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, falls under the directive EU2016/680.

### 2.2 Application of the Law Enforcement Directive, LED (EU2016/680)

11. Pursuant to Article 2 (2) (c), the processing of personal data by a natural person in the course of a purely personal or household activity, which can also include online activity, is out of the scope of the GDPR.<sup>3</sup>
12. This provision – the so-called household exemption – in the context of video surveillance must be narrowly construed. Hence, as considered by the European Court of Justice, the so called "household

---

<sup>2</sup> The EDPB notes that where the GDPR so allows, specific requirements in national legislation might apply.

<sup>3</sup> See also Recital 18.

exemption" must "be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people".<sup>4</sup> Furthermore, if a video surveillance system, to the extent it involves the constant recording and storage of personal data and covers, "even partially, a public space and is accordingly directed outwards from the private setting of the person processing the data in that manner, it cannot be regarded as an activity which is a purely 'personal or household' activity for the purposes of the second indent of Article 3(2) of Directive 95/46"<sup>5</sup>.

13. What regards video devices operated inside a private person's premises, it may fall under the household exemption. It will depend on several factors, which all have to be considered in order to reach a conclusion. Besides the above mentioned elements identified by ECJ rulings, the user of video surveillance at home needs to look at whether he has some kind of personal relationship with the data subject, whether the scale or frequency of the surveillance suggests some kind of professional activity on his side, and of the surveillance's potential adverse impact on the data subjects. The presence of any single one of the aforementioned elements does not necessarily suggest that the processing is outside the scope of the household exemption, an overall assessment is needed for that determination.

Example: A tourist is recording videos both through his mobile phone and through a camcorder to document his holidays. He shows the footage to friends and family but does not make it accessible for an indefinite number of people. This would fall under the household exemption.

Example: A downhill mountain biker wants to record her descent with an actioncam. She is riding in a remote area and only plans to use the recordings for her personal entertainment at home. This would fall under the household exemption even if to some extent personal data is processed.

Example: Somebody is monitoring and recording his own garden. The property is fenced and only the controller himself and his family are entering the garden on a regular basis. This would fall under the household exemption, provided that the video surveillance does not extend even partially to a public space or neighbouring property.

- 14.

---

<sup>4</sup> European Court of Justice, Judgment in Case C-101/01, *Bodil Lindqvist case*, 6th November 2003, para 47.

<sup>5</sup> European Court of Justice, Judgment in Case C-212/13, *František Ryneš v Úřad pro ochranu osobních údajů*, 11 December 2014, para. 33.

### 3 LAWFULNESS OF PROCESSING

15. Before use, the purposes of processing have to be specified in detail (Article 5 (1) (b)). Video surveillance can serve many purposes, e.g. supporting the protection of property and other assets, supporting the protection of life and physical integrity of individuals, collecting evidence for civil claims.<sup>6</sup> These monitoring purposes should be documented in writing (Article 5 (2)) and need to be specified for every surveillance camera in use. Cameras that are used for the same purpose by a single controller can be documented together. Furthermore, data subjects must be informed of the purpose(s) of the processing in accordance with Article 13 (see section 7, Transparency and information obligations). Video surveillance based on the mere purpose of “safety” or “for your safety” is not sufficiently specific (Article 5 (1) (b)). It is furthermore contrary to the principle that personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (see Article 5 (1) (a)).
16. In principle, every legal ground under Article 6 (1) can provide a legal basis for processing video surveillance data. For example, Article 6 (1) (c) applies where national law stipulates an obligation to carry out video surveillance.<sup>7</sup> However in practice, the provisions most likely to be used are
  - Article 6 (1) (f) (legitimate interest),
  - Article 6 (1) (e) (necessity to perform a task carried out in the public interest or in the exercise of official authority).

In rather exceptional cases Article 6 (1) (a) (consent) might be used as a legal basis by the controller.

#### 3.1 Legitimate interest, Article 6 (1) (f)

17. The legal assessment of Article 6 (1) (f) should be based on the following criteria in compliance with Recital 47.
  - 18.1 **3.1.1 Existence of legitimate interests** Video surveillance is lawful if it is necessary in order to meet the purpose of a legitimate interest pursued by a controller or a third party, unless such interests are overridden by the data subject's interests or fundamental rights and freedoms (Article 6 (1) (f)). Legitimate interests pursued by a controller or a third party can be legal<sup>8</sup>, economic or non-material interests.<sup>9</sup> However, the controller should consider that if the data subject objects to the surveillance in accordance with Article 21 the controller can only proceed with the video surveillance of that data subject if it is a *compelling* legitimate interest which overrides the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.
  19. Given a real and hazardous situation, the purpose to protect property against burglary, theft or vandalism can constitute a legitimate interest for video surveillance.

---

<sup>6</sup> Rules on collecting evidence for civil claims varies in Member States.

<sup>7</sup> These guidelines do not analyse or go into details of national law that might differ between Member States.

<sup>8</sup> European Court of Justice, Judgment in Case C-13/16, *Rīgas satiksme case*, 4 may 2017

<sup>9</sup> see WP217, Article 29 Working Party.

20. The legitimate interest needs to be of real existence and has to be a present issue (i.e. it must not be fictional or speculative)<sup>10</sup>. A real-life situation of distress needs to be at hand – such as damages or serious incidents in the past – before starting the surveillance. In light of the principle of accountability, controllers would be well advised to document relevant incidents (date, manner, financial loss) and related criminal charges. Those documented incidents can be a strong evidence for the existence of a legitimate interest. The existence of a legitimate interest as well as the necessity of the monitoring should be reassessed in periodic intervals (e. g. once a year, depending on the circumstances).

**Example:** A shop owner wants to open a new shop and wants to install a video surveillance system to prevent vandalism. He can show, by presenting statistics, that there is a high expectation of vandalism in the near neighbourhood. Also, experience from neighbouring shops is useful. It is not necessary that a damage to the controller in question must have occurred. As long as damages in the neighbourhood suggest a danger or similar, and thus can be an indication of a legitimate interest. It is however not sufficient to present national or general crime statistic without analysing the area in question or the dangers for this specific shop.

- 21.
22. Imminent danger situations may constitute a legitimate interest, such as banks or shops selling precious goods (e.g. jewellers), or areas that are known to be typical crime scenes for property offences (e. g. petrol stations).
23. The GDPR also clearly states that public authorities cannot rely their processing on the grounds of legitimate interest, as long as they are carrying out their tasks, Article 6 (1) sentence 2.

### 3.1.2 Necessity of processing

24. Personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'), see Article 5 (1) (c). Before installing a video-surveillance system the controller should always critically examine if this measure is firstly suitable to attain the desired goal, and secondly adequate and necessary for its purposes. Video surveillance measures should only be chosen if the purpose of the processing could not reasonably be fulfilled by other means which are less intrusive to the fundamental rights and freedoms of the data subject.
25. Given the situation that a controller wants to prevent property related crimes, instead of installing a video surveillance system the controller could also take alternative security measures such as fencing the property, installing regular patrols of security personnel, using gatekeepers, providing better lighting, installing security locks, tamper-proof windows and doors or applying anti-graffiti coating or foils to walls. Those measures can be as effective as video surveillance systems against burglary, theft and vandalism. The controller has to assess on a case-by-case basis whether such measures can be a reasonable solution.
26. Before operating a camera system, the controller is obliged to assess where and when video surveillance measures are strictly necessary. Usually a surveillance system operating at night-time as well as outside the regular working hours will meet the needs of the controller to prevent any dangers to his property.

---

<sup>10</sup> see WP217, Article 29 Working Party, p. 24 seq. See also ECJ Case C-708/18 p.44

27. In general, the necessity to use video surveillance to protect the controllers' premises ends at the property boundaries.<sup>11</sup> However, there are cases where the surveillance of the property is not sufficient for an effective protection. In some individual cases it might be necessary to exceed the video surveillance to the immediate surroundings of the premises. In this context, the controller should consider physical and technical means, for example blocking out or pixelating not relevant areas.

**Example:** A bookshop wants to protect its premises against vandalism. In general, cameras should only be filming the premises itself because it is not necessary to watch neighbouring premises or public areas in the surrounding of the bookshop premises for that purpose.

- 28.
29. Questions concerning the processing's necessity also arise regarding the way evidence is preserved. In some cases it might be necessary to use black box solutions where the footage is automatically deleted after a certain storage period and only accessed in case of an incident. In other situations, it might not be necessary to record the video material at all but more appropriate to use real-time monitoring instead. The decision between black box solutions and real-time monitoring should also be based on the purpose pursued. If for example the purpose of video surveillance is the preservation of evidence, real-time methods are usually not suitable. Sometimes real-time monitoring may also be more intrusive than storing and automatically deleting material after a limited timeframe (e. g. if someone is constantly viewing the monitor it might be more intrusive than if there is no monitor at all and material is directly stored in a black box). The data minimisation principle must be regarded in this context (Article 5 (1) (c)). It should also be kept in mind that it might be possible that the controller could use security personnel instead of video surveillance that are able to react and intervene immediately.

### 3.1.3 Balancing of interests

30. Presuming that video surveillance is necessary to protect the legitimate interests of a controller, a video surveillance system may only be put in operation, if the legitimate interests of the controller or those of a third party (e.g. protection of property or physical integrity) are not overridden by the interests or fundamental rights and freedoms of the data subject. The controller needs to consider 1) to what extent the monitoring affects interests, fundamental rights and freedoms of individuals and 2) if this causes violations or negative consequences with regard to the data subject's rights. In fact, balancing the interests is mandatory. Fundamental rights and freedoms on one hand and the controller's legitimate interests on the other hand have to be evaluated and balanced carefully.

---

<sup>11</sup> This might also be subject to national legislation in some Member States.

Example: A private parking company has documented reoccurring problems with thefts in the cars parked. The parking area is an open space and can be easily accessed by anyone, but is clearly marked with signs and road blockers surrounding the space. The parking company have a legitimate interest (preventing thefts in the customers' cars) to monitor the area during the time of day that they are experiencing problems. Data subjects are monitored in a limited timeframe, they are not in the area for recreational purposes and it is also in their own interest that thefts are prevented. The interest of the data subjects not to be monitored is in this case overridden by the controller's legitimate interest.

Example: A restaurant decides to install video cameras in the restrooms to control the tidiness of the sanitary facilities. In this case the rights of the data subjects clearly overrides the interest of the controller, therefore cameras cannot be installed there.

31.

#### *3.1.3.1 Making case-by-case decisions*

32. As the balancing of interests is mandatory according to the regulation, the decision has to be made on a case-by-case basis (see Article 6 (1) (f)). Referencing abstract situations or comparing similar cases to one another is insufficient. The controller has to evaluate the risks of the intrusion of the data subject's rights; here the decisive criterion is the intensity of intervention for the rights and freedoms of the individual.
33. Intensity can inter alia be defined by the type of information that is gathered (information content), the scope (information density, spatial and geographical extent), the number of data subjects concerned, either as a specific number or as a proportion of the relevant population, the situation in question, the actual interests of the group of data subjects, alternative means, as well as by the nature and scope of the data assessment.
34. Important balancing factors can be the size of the area, which is under surveillance and the amount of data subjects under surveillance. The use of video surveillance in a remote area (e. g. to watch wildlife or to protect critical infrastructure such as a privately owned radio antenna) has to be assessed differently than video surveillance in a pedestrian zone or a shopping mall.

Example: If a dash cam is installed (e. g. for the purpose of collecting evidence in case of an accident), it is important to ensure that this camera is not constantly recording traffic, as well as persons who are near a road. Otherwise the interest in having video recordings as evidence in the more theoretical case of a road accident cannot justify this serious interference with data subjects' rights.<sup>11</sup>

35.

#### *3.1.3.2 Data subjects' reasonable expectations*

36. According to Recital 47, the existence of a legitimate interest needs careful assessment. Here the reasonable expectations of the data subject at the time and in the context of the processing of its personal data have to be included. Concerning systematic monitoring, the relationship between data subject and controller may vary significantly and may affect what reasonable expectations the data subject might have. The interpretation of the concept of reasonable expectations should not only be based on the subjective expectations in question. Rather, the decisive criterion has to be if an objective third party could reasonably expect and conclude to be subject to monitoring in this specific situation.

37. For instance, an employee in his/her workplace is in most cases not likely expecting to be monitored by his or her employer.<sup>12</sup> Furthermore, monitoring is not to be expected in one's private garden, in living areas, or in examination and treatment rooms. In the same vein, it is not reasonable to expect monitoring in sanitary or sauna facilities – monitoring such areas is an intense intrusion into the rights of the data subject. The reasonable expectations of data subjects are that no video surveillance will take place in those areas. On the other hand, the customer of a bank might expect that he/she is monitored inside the bank or by the ATM.
38. Data subjects can also expect to be free of monitoring within publicly accessible areas especially if those areas are typically used for recovery, regeneration, and leisure activities as well as in places where individuals stay and/or communicate, such as sitting areas, tables in restaurants, parks, cinemas and fitness facilities. Here the interests or rights and freedoms of the data subject will often override the controller's legitimate interests.

Example: In toilets data subjects expect not to be monitored. Video surveillance for example to prevent accidents is not proportional.

- 39.
40. Signs informing the data subject about the video surveillance have no relevance when determining what a data subject objectively can expect. This means that e.g. a shop owner cannot rely on customers *objectively* having reasonable expectations to be monitored just because a sign informs the individual at the entrance about the surveillance.

### 3.2 Necessity to perform a task carried out in the public interest or in the exercise of official authority vested in the controller, Article 6 (1) (e)

41. Personal data could be processed through video surveillance under Article 6 (1) (e) if it is necessary to perform a task carried out in the public interest or in the exercise of official authority.<sup>13</sup> It may be that the exercise of official authority does not allow for such processing, but other legislative bases such as "health and safety" for the protection of visitors and employees may provide limited scope for processing, while still having regard for GDPR obligations and data subject rights.
42. Member States may maintain or introduce specific national legislation for video surveillance to adapt the application of the rules of the GDPR by determining more precisely specific requirements for processing as long as it is in accordance with the principles laid down by the GDPR (e.g. storage limitation, proportionality).

---

<sup>12</sup> See also: Article 29 Working Party, Opinion 2/2017 on data processing at work, WP249, adopted on 8 June 2017.

<sup>13</sup> The basis for the processing referred shall be laid down by Union law or Member State law» and «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 (Article 6 (3)).

### 3.3 Consent, Article 6 (1) (a)

43. Consent has to be freely given, specific, informed and unambiguous as described in the guidelines on consent.<sup>14</sup>
44. Regarding systematic monitoring, the data subject's consent can only serve as a legal basis in accordance with Article 7 (see Recital 43) in exceptional cases. It is in the surveillance's nature that this technology monitors an unknown number of people at once. The controller will hardly be able to prove that the data subject has given consent prior to processing of its personal data (Article 7 (1)). Assumed that the data subject withdraws its consent it will be difficult for the controller to prove that personal data is no longer processed (Article 7 (3)).

Example: Athletes may request monitoring during individual exercises in order to analyse their techniques and performance. On the other hand, where a sports club takes the initiative to monitor a whole team for the same purpose, consent will often not be valid, as the individual athletes may feel pressured into giving consent so that their refusal of consent does not adversely affect teammates.

- 45.
46. If the controller wishes to rely on consent it is his duty to make sure that every data subject who enters the area which is under video surveillance has given her or his consent. This consent has to meet the conditions of Article 7. Entering a marked monitored area (e.g. people are invited to go through a specific hallway or gate to enter a monitored area), does not constitute a statement or a clear affirmative action needed for consent, unless it meets the criteria of Article 4 and 7 as described in the guidelines on consent.<sup>15</sup>
47. Given the imbalance of power between employers and employees, in most cases employers should not rely on consent when processing personal data, as it is unlikely to be freely given. The guidelines on consent should be taken into consideration in this context.
48. Member State law or collective agreements, including 'works agreements', may provide for specific rules on the processing of employees' personal data in the employment context (see Article 88).

---

<sup>14</sup> Article 29 Working Party (Art. 29 WP) „Guidelines on consent under Regulation 2016/679“ (WP 259 rev. 01). - endorsed by the EDPB

<sup>15</sup> Article 29 Working Party (Art. 29 WP) „Guidelines on consent under Regulation 2016/679“ (WP 259) - endorsed by the EDPB - which should be taken in account.

## 4 DISCLOSURE OF VIDEO FOOTAGE TO THIRD PARTIES

49. In principle, the general regulations of the GDPR apply to the disclosure of video recordings to third parties.

### 4.1 Disclosure of video footage to third parties in general

50. Disclosure is defined in Article 4 (2) as transmission (e.g. individual communication), dissemination (e.g. publishing online) or otherwise making available. Third parties are defined in Article 4 (10). Where disclosure is made to third countries or international organisations, the special provisions of Article 44 et seq. also apply.

51. Any disclosure of personal data is a separate kind of processing of personal data for which the controller needs to have a legal basis in Article 6.

Example: A controller who wishes to upload a recording to the Internet needs to rely on a legal basis for that processing, for instance by obtaining consent from the data subject according to Article 6 (1) (a).

52.

53. The transmission of video footage to third parties for the purpose other than that for which the data has been collected is possible under the rules of Article 6 (4).

Example: Video surveillance of a barrier (at a parking lot) is installed for the purpose of resolving damages. A damage occurs and the recording is transferred to a lawyer to pursue a case. In this case the purpose for recording is the same as the one for transferring.

Example: Video surveillance of a barrier (at a parking lot) is installed for the purpose of resolving damages. The recording is published online for pure amusement reasons. In this case the purpose has changed and is not compatible with the initial purpose. It would furthermore be problematic to identify a legal basis for that processing (publishing).

54.

55. A third party recipient will have to make its own legal analysis, in particular identifying its legal basis under Article 6 for his processing (e.g. receiving the material).

### 4.2 Disclosure of video footage to law enforcement agencies

56. The disclosure of video recordings to law enforcement agencies is also an independent process, which requires a separate justification for the controller.

57. According to Article 6 (1) (c), processing is legal if it is necessary for compliance with a legal obligation to which the controller is subject. Although the applicable police law is an affair under the sole control of the Member States, there are most likely general rules that regulate the transfer of evidence to law enforcement agencies in every Member State. The processing of the controller handing over the data is regulated by the GDPR. If national legislation requires the controller to cooperate with law enforcement (e. g. investigation), the legal basis for handing over the data is legal obligation under Article 6 (1) (c).

58. The purpose limitation in Article 6 (4) is then often unproblematic, since the disclosure explicitly goes back to Member State law. A consideration of the special requirements for a change of purpose in the sense of lit. a - e is therefore not necessary.

Example: A shop owner records footage at its entrance. The footage shows a person stealing another person's wallet. The police asks the controller to hand over the material in order to assist in their investigation. In that case the shop owner would use the legal basis under Article 6 (1) (c) (legal obligation) read in conjunction with the relevant national law for the transfer processing.

59.

Example: A camera is installed in a shop for security reasons. The shop owner believes he has recorded something suspicious in his footage and decides to send the material to the police (without any indication that there is an ongoing investigation of some kind). In this case the shop owner has to assess whether the conditions under, in most cases, Article 6 (1) (f) are met. This is usually the case if the shop owner has a reasonable suspicion of that a crime has been committed.

60.

61. The processing of the personal data by the law enforcement agencies themselves does not follow the GDPR (see Article 2 (2) (d)), but follows instead the Law Enforcement Directive (EU2016/680).

## 5 PROCESSING OF SPECIAL CATEGORIES OF DATA

62. Video surveillance systems usually collect massive amounts of personal data which may reveal data of a highly personal nature and even special categories of data. Indeed, apparently non-significant data originally collected through video can be used to infer other information to achieve a different purpose (e.g. to map an individual's habits). However, video surveillance is not always considered to be processing of special categories of personal data.

Example: Video footage showing a data subject wearing glasses or using a wheel chair are not per se considered to be special categories of personal data.

63.

64. However, if the video footage is processed to deduce special categories of data Article 9 applies.

Example: Political opinions could for example be deduced from images showing identifiable data subjects taking part in an event, engaging in a strike, etc. This would fall under Article 9.

Example: A hospital installing a video camera in order to monitor a patient's health condition would be considered as processing of special categories of personal data (Article 9).

65.

66. In general, as a principle, whenever installing a video surveillance system careful consideration should be given to the data minimization principle. Hence, even in cases where Article 9 (1) does not apply, the data controller should always try to minimize the risk of capturing footage revealing other sensitive data (beyond Article 9), regardless of the aim.

Example: Video surveillance capturing a church does not per se fall under Article 9. However, the controller has to conduct an especially careful assessment under Article 6 (1) (f) taken into account the nature of the data as well as the risk of capturing other sensitive data (beyond Article 9) when assessing the interests of the data subject.

67.

68. If a video surveillance system is used in order to process special categories of data, the data controller must identify both an exception for processing special categories of data under Article 9 (i.e. an exemption from the general rule that one should not process special categories of data) and a legal basis under Article 6.

69. For instance, Article 9 (2) (c) ("[...] *processing is necessary to protect the vital interests of the data subject or of another natural person [...]*") could – in theory and exceptionally – be used, but the data controller would have to justify it as an absolute necessity to safeguard the vital interests of a person and prove that this "[...] *data subject is physically or legally incapable of giving his consent.*". In addition, the data controller won't be allowed to use the system for any other reason.

70. It is important to note here that every exemption listed in Article 9 is not likely to be usable to justify processing of special categories of data through video surveillance. More specifically, data controllers processing those data in the context of video surveillance cannot rely on Article 9 (2) (e), which allows processing that relates to personal data that are manifestly made public by the data subject. The mere fact of entering into the range of the camera does not imply that the data subject intends to make public special categories of data relating to him or her.

71. Furthermore, processing of special categories of data requires a heightened and continued vigilance to certain obligations; for example high level of security and data protection impact assessment where necessary.

Example: An employer must not use video surveillance recordings showing a demonstration in order to identify strikers.

72.

### 5.1 General considerations when processing biometric data

73. The use of biometric data and in particular facial recognition entail heightened risks for data subjects' rights. It is crucial that recourse to such technologies takes place with due respect to the principles of lawfulness, necessity, proportionality and data minimisation as set forth in the GDPR. Whereas the use of these technologies can be perceived as particularly effective, controllers should first of all assess the impact on fundamental rights and freedoms and consider less intrusive means to achieve their legitimate purpose of the processing.
74. To qualify as biometric data as defined in the GDPR, processing of raw data, such as the physical, physiological or behavioural characteristics of a natural person, must imply a measurement of this characteristics. Since biometric data is the result of such measurements, the GDPR states in its Article 4.14 that it is “[...] *resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person [...]*”. The video footage of an individual cannot however in itself be considered as biometric data under Article 9, if it has not been specifically technically processed in order to contribute to the identification of an individual.<sup>16</sup>
75. In order for it to be considered as processing of special categories of personal data (Article 9) it requires that biometric data is processed “for the purpose of uniquely identifying a natural person”.
76. To sum up, in light of Article 4.14 and 9, three criteria must be considered:
- **Nature of data :** data relating to physical, physiological or behavioural characteristics of a natural person,
  - **Means and way of processing :** data “resulting from a specific technical processing”,
  - **Purpose of processing:** data must be used for the purpose of uniquely identifying a natural person.
77. The use of video surveillance including biometric recognition functionality installed by private entities for their own purposes (e.g. marketing, statistical, or even security) will, in most cases, require explicit consent from all data subjects (Article 9 (2) (a)), however another suitable exception in Article 9 could also be applicable.

---

<sup>16</sup> Recital 51 GDPR supports this analysis, stating that “[...] *The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. [...]*”.

Example: To improve its service a private company replaces passenger identification check points within an airport (luggage drop-off, boarding) with video surveillance systems that use facial recognition techniques to verify the identity of the passengers that have chosen to consent to such a procedure. Since the processing falls under Article 9, the passengers, who will have previously given their explicit and informed consent, will have to enlist themselves at for example an automatic terminal in order to create and register their facial template associated with their boarding pass and identity. The check points with facial recognition need to be clearly separated, e. g. the system must be installed within a gantry so that the biometric templates of non-consenting person will not be captured. Only the passengers, who will have previously given their consent and proceeded with their enrolment, will use the gantry equipped with the biometric system.

Example: A controller manages access to his building using a facial recognition method. People can only use this way of access if they have given their explicitly informed consent (according to Article 9 (2) (a)) beforehand. However, in order to ensure that no one who has not previously given his or her consent is captured, the facial recognition method should be triggered by the data subject himself, for instance by pushing a button. To ensure the lawfulness of the processing, the controller must always offer an alternative way to access the building, without biometric processing, such as badges or keys.

- 78.
79. In this type of cases, where biometric templates are generated, controllers shall ensure that once a match or no-match result has been obtained, all the intermediate templates made on the fly (with the explicit and informed consent of the data subject) in order to be compared to the ones created by the data subjects at the time of the enlistment, are immediately and securely deleted. The templates created for the enlistment should only be retained for the realisation of the purpose of the processing and should not be stored or archived.
80. However, when the purpose of the processing is for example to distinguish one category of people from another but not to uniquely identify anyone the processing does not fall under Article 9.

Example: A shop owner would like to customize its advertisement based on gender and age characteristics of the customer captured by a video surveillance system. If that system does not generate biometric templates in order to uniquely identify persons but instead just detects those physical characteristics in order to classify the person then the processing would not fall under Article 9 (as long as no other types of special categories of data are being processed).

- 81.
82. However, Article 9 applies if the controller stores biometric data (most commonly through templates that are created by the extraction of key features from the raw form of biometric data (e.g. facial measurements from an image)) in order to uniquely identify a person. If a controller wishes to detect a data subject re-entering the area or entering another area (for example in order to project continued customized advertisement), the purpose would then be to uniquely identify a natural person, meaning that the operation would from the start fall under Article 9. This could be the case if a controller stores generated templates to provide further tailored advertisement on several billboards throughout different locations inside the shop. Since the system is using physical characteristics to detect specific individuals coming back in the range of the camera (like the visitors of a shopping mall) and tracking them, it would constitute a biometric identification method because it is aimed at recognition through the use of specific technical processing.

- Example: A shop owner has installed a facial recognition system inside his shop in order to customize its advertisement towards individuals. The data controller has to obtain the explicit and informed consent of all data subjects before using this biometric system and delivering tailored advertisement. The system would be unlawful if it captures visitors or passers-by who have not consented to the creation of their biometric template, even if their template is deleted within the shortest possible period. Indeed, these temporary templates constitute biometric data processed in order to uniquely identify a person who may not want to receive targeted advertisement.
- 83.
84. The EDPB observes that some biometric systems are installed in uncontrolled environments<sup>17</sup>, which means that the system involves capturing on the fly the faces of any individual passing in the range of the camera, including persons who have not consented to the biometric device, and thereby creating biometric templates. These templates are compared to the ones created of data subjects having given their prior consent during an enlistment process (i.e. a biometric devise user) in order for the data controller to recognise whether the person is a biometric device user or not. In this case, the system is often designed to discriminate the individuals it wants to recognize from a database from those who are not enlisted. Since the purpose is to uniquely identify natural persons, an exception under Article 9 (2) GDPR is still needed for anyone captured by the camera.
- Example: A hotel uses video surveillance to automatically alert the hotel manager that a VIP has arrived when the face of the guest is recognized. These VIPs have priority given their explicit consent to the use of facial recognition before being recorded in a database established for that purpose. These processing systems of biometric data would be unlawful unless all other guests monitored (in order to identify the VIPs) have consented to the processing according to Article 9 (2) (a) GDPR.
- Example: A controller installs a video surveillance system with facial recognition at the entrance of the concert hall he manages. The controller must set up clearly separated entrances; one with a biometric system and one without (where you instead for example scan a ticket). The entrances equipped with biometric devices, must be installed and made accessible in a way that prevents the system from capturing biometric templates of non-consenting spectators.
- 85.
86. Finally, when the consent is required by Article 9 GDPR, the data controller shall not condition the access to its services to the acceptance of the biometric processing. In other words and notably when the biometric processing is used for authentication purpose, the data controller must offer an alternative solution that does not involve biometric processing – without restraints or additional cost for the data subject. This alternative solution is also needed for persons who do not meet the constraints of the biometric device (enrolment or reading of the biometric data impossible, disability situation making it difficult to use, etc.) and in anticipation of unavailability of the biometric device (such as a malfunction of the device), a "back-up solution" must be implemented to ensure continuity of the proposed service, limited however to exceptional use. In exceptional cases, there might be a situation where processing biometric data is the core activity of a service provided by contract, e.g. a

---

<sup>17</sup> It means that the biometric device is located in a space open to the public and is able to work on anyone passing by, as opposed to the biometric systems in controlled environments that can be used only by consenting person's participation.

museum that sets up an exhibition to demonstrate the use of a facial recognition device, in which case the data subject will not be able to reject the processing of biometric data should they wish to participate in the exhibition. In such case the consent required under Article 9 is still valid if the requirements in Article 7 are met.

## 5.2 Suggested measures to minimize the risks when processing biometric data

87. In compliance with the data minimization principle, data controllers must ensure that data extracted from a digital image to build a template will not be excessive and will only contain the information required for the specified purpose, thereby avoiding any possible further processing. Measures should be put in place to guarantee that templates cannot be transferred across biometric systems.
88. Identification and authentication/verification are likely to require the storage of the template for use in a later comparison. The data controller must consider the most appropriate location for storage of the data. In an environment under control (delimited hallways or checkpoints), templates shall be stored on an individual device kept by the user and under his or her sole control (in a smartphone or the id card) or – when needed for specific purposes and in presence of objective needs – stored in a centralized database in an encrypted form with a key/secret solely in the hands of the person to prevent unauthorised access to the template or storage location. If the data controller cannot avoid having access to the templates, he must take appropriate steps to ensure the security of the data stored. This may include encrypting the template using a cryptographic algorithm.
89. In any case, the controller shall take all necessary precautions to preserve the availability, integrity and confidentiality of the data processed. To this end, the controller shall notably take the following measures: compartmentalize data during transmission and storage, store biometric templates and raw data or identity data on distinct databases, encrypt biometric data, notably biometric templates, and define a policy for encryption and key management, integrate an organisational and technical measure for fraud detection, associate an integrity code with the data (for example signature or hash) and prohibit any external access to the biometric data. Such measures will need to evolve with the advancement of technologies.
90. Besides, data controllers should proceed to the deletion of raw data (face images, speech signals, the gait, etc.) and ensure the effectiveness of this deletion. If there is no longer a lawful basis for the processing, the raw data has to be deleted. Indeed, insofar as biometric templates derives from such data, one can consider that the constitution of databases could represent an equal if not even bigger threat (because it may not always be easy to read a biometric template without the knowledge of how it was programmed, whereas raw data will be the building blocks of any template). In case the data controller would need to keep such data, noise-additive methods (such as watermarking) must be explored, which would render the creation of the template ineffective. The controller must also delete biometric data and templates in the event of unauthorized access to the read-comparison terminal or storage server and delete any data not useful for further processing at the end of the biometric device's life.

## 6 RIGHTS OF THE DATA SUBJECT

91. Due to the character of data processing when using video surveillance some data subject's rights under GDPR serves further clarification. This chapter is however not exhaustive, all rights under the GDPR applies to processing of personal data through video surveillance.

### 6.1 Right to access

92. A data subject has the right to obtain confirmation from the controller as to whether or not their personal data are being processed. For video surveillance this means that if no data is stored or transferred in any way then once the real-time monitoring moment has passed the controller could only give the information that no personal data is any longer being processed (besides the general information obligations under Article 13, see *section 7 – Transparency and information obligations*). If however data is still being processed at the time of the request (i.e. if the data is stored or continuously processed in any other way), the data subject should receive access and information in accordance with Article 15.
93. There are however, a number of limitations that may in some cases apply in relation to the right to access.
- Article 15 (4) GDPR, adversely affect the rights of others
94. Given that any number of data subjects may be recorded in the same sequence of video surveillance a screening would then cause additional processing of personal data of other data subjects. If the data subject wishes to receive a copy of the material (article 15 (3)), this could adversely affect the rights and freedoms of other data subject in the material. To prevent that effect the controller should therefore take into consideration that due to the intrusive nature of the video footage the controller should not in some cases hand out video footage where other data subjects can be identified. The protection of the rights of third parties should however not be used as an excuse to prevent legitimate claims of access by individuals, the controller should in those cases implement technical measures to fulfil the access request (for example, image-editing such as masking or scrambling). However, controllers are not obliged to implement such technical measures if they can otherwise ensure that they are able to react upon a request under Article 15 within the timeframe stipulated by Article 12 (3).
- Article 11 (2) GDPR, controller is unable to identify the data subject
95. If the video footage is not searchable for personal data, (i.e. the controller would likely have to go through a large amount of stored material in order to find the data subject in question) the controller may be unable to identify the data subject.
96. For these reasons the data subject should (besides identifying themselves including with identification document or in person) in its request to the controller, specify when – within a reasonable timeframe in proportion to the amount of data subjects recorded – he or she entered the monitored area. The controller should notify the data subject beforehand on what information is needed in order for the controller to comply with the request. If the controller is able to demonstrate that it is not in a position to identify the data subject, the controller must inform the data subject accordingly, if possible. In such a situation, in its response to the data subject the controller should inform about the exact area for the monitoring, verification of cameras that were in use etc. so that the data subject will have the full understanding of what personal data of him/her may have been processed.

Example: If a data subject is requesting a copy of his or her personal data processed through video surveillance at the entrance of a shopping mall with 30 000 visitors per day, the data subject should specify when he or she passed the monitored area within approximately a one-hour-timeframe. If the controller still processes the material a copy of the video footage should be provided. If other data subjects can be identified in the same material then that part of the material should be anonymised (for example by blurring the copy or parts thereof) before giving the copy to the data subject that filed the request.

Example: If the controller is automatically erasing all footage for example within 2 days, the controller is not able to supply footage to the data subject after those 2 days. If the controller receives a request after those 2 days the data subject should be informed accordingly.

97.

- Article 12 GDPR, excessive requests

98.

In case of excessive or manifestly unfounded requests from a data subject, the controller may either charge a reasonable fee in accordance with Article 12 (5) (a) GDPR, or refuse to act on the request (Article 12 (5) (b) GDPR). The controller needs to be able to demonstrate the manifestly unfounded or excessive character of the request.

## 6.2 Right to erasure and right to object

### 6.2.1 Right to erasure (Right to be forgotten)

99. If the controller continues to process personal data beyond real-time monitoring (e.g. storing) the data subject may request for the personal data to be erased under Article 17 GDPR.

100. Upon a request, the controller is obliged to erase the personal data without undue delay if one of the circumstances listed under Article 17 (1) GDPR applies (and none of the exceptions listed under Article 17 (3) GDPR does). That includes the obligation to erase personal data when they are no longer needed for the purpose for which they were initially stored, or when the processing is unlawful (see also *Section 8 – Storage periods and obligation to erasure*). Furthermore, depending on the legal basis of processing, personal data should be erased:

- for consent whenever the consent is withdrawn (and there is no other legal basis for the processing)
- for legitimate interest:
  - whenever the data subject exercises the right to object (see *Section 6.2.2*) and there are no overriding compelling legitimate grounds for the processing, or
  - in case of direct marketing (including profiling) whenever the data subject objects to the processing.

101. If the controller has made the video footage public (e.g. broadcasting or streaming online), reasonable steps need to be taken in order to inform other controllers (that are now processing the personal data in question) of the request pursuant to Article 17 (2) GDPR. The reasonable steps should include technical measures, taking into account available technology and the cost of implementation. To the extent possible, the controller should notify – upon erasure of personal data – anyone to which the personal data previously have been disclosed, in accordance with Article 19 GDPR.

102. Besides the controller's obligation to erase personal data upon the data subject's request, the controller is obliged under the general principles of the GDPR to limit the personal data stored (see *Section 8*).
103. For video surveillance it is worth noticing that by for instance blurring the picture with no retroactive ability to recover the personal data that the picture previously contained, the personal data are considered erased in accordance with GDPR.

**Example:** A convenience store is having trouble with vandalism in particular on its exterior and is therefore using video surveillance outside of their entrance in direct connection to the walls. A passer-by requests to have his personal data erased from that very moment. The controller is obliged to respond to the request without undue delay and at the latest within one month. Since the footage in question does no longer meet the purpose for which it was initially stored (no vandalism occurred during the time the data subject passed by), there is at the time of the request, no legitimate interest to store the data that would override the interests of the data subjects. The controller needs to erase the personal data.

104.

#### 6.2.2 Right to object

105. For video surveillance based on *legitimate interest* (Article 6 (1) (f) GDPR) or for the necessity when carrying out a task in the *public interest* (Article 6 (1) (e) GDPR) the data subject has the right – at any time – to object, on grounds relating to his or her particular situation, to the processing in accordance with Article 21 GDPR. Unless the controller demonstrates compelling legitimate grounds that overrides the rights and interests of the data subject, the processing of data of the individual who objected must then stop. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month.
106. In the context of video surveillance this objection could be made either when entering, during the time in, or after leaving, the monitored area. In practice this means that unless the controller has compelling legitimate grounds, monitoring an area where natural persons could be identified is only lawful if either
  - (1) the controller is able to immediately stop the camera from processing personal data when requested, or
  - (2) the monitored area is in such detail restricted so that the controller can assure the approval from the data subject prior to entering the area and it is not an area that the data subject as a citizen is entitled to access.
107. These guidelines do not aim to identify what is considered a *compelling legitimate interest* (Article 21 GDPR).
108. When using video surveillance for direct marketing purposes, the data subject has the right to object to the processing on a discretionary basis as the right to object is absolute in that context (Article 21 (2) and (3) GDPR).

Example: A company is experiencing difficulties with security breaches in their public entrance and is using video surveillance on the grounds of legitimate interest, with the purpose to catch those unlawfully entering. A visitor objects to the processing of his or her data through the video surveillance system on grounds relating to his or her particular situation. The company however in this case rejects the request with the explanation that the footage stored is needed due to an ongoing internal investigation, thereby having compelling legitimate grounds to continue processing the personal data.

109.

## 7 TRANSPARENCY AND INFORMATION OBLIGATIONS<sup>18</sup>

110. It has long been inherent in European data protection law that data subjects should be aware of the fact that video surveillance is in operation. They should be informed in a detailed manner as to the places monitored.<sup>19</sup> Under the GDPR the general transparency and information obligations are set out in Article 12 GDPR and following. Article 29 Working Party's "Guidelines on transparency under Regulation 2016/679 (WP260)" which were endorsed by the EDPB on May 25<sup>th</sup> 2018 provide further details. In line with WP260 par. 26, it is Article 13 GDPR, which is applicable if personal data are collected "[...] from a data subject by observation (e.g. using automated data capturing devices or data capturing software such as cameras [...])."
111. In light of the volume of information, which is required to be provided to the data subject, a layered approach may be followed by data controllers where they opt to use a combination of methods to ensure transparency (WP260, par. 35; WP89, par. 22). Regarding video surveillance the most important information should be displayed on the warning sign itself (first layer) while the further mandatory details may be provided by other means (second layer).

### 7.1 First layer information (warning sign)

112. The first layer concerns the primary way in which the controller first engages with the data subject. At this stage, controllers may use a warning sign showing the relevant information. The displayed information may be provided in combination with an icon in order to give, in an easily visible, intelligible and clearly readable manner, a meaningful overview of the intended processing (Article 12 (7) GDPR). The format of the information should be adjusted to the individual location (WP89 par. 22).

#### 7.1.1 Positioning of the warning sign

113. The information should be positioned in such a way that the data subject can easily recognize the circumstances of the surveillance before entering the monitored area (approximately at eye level). It is not necessary to reveal the position of the camera as long as there is no doubt as to which areas are subject to monitoring and the context of surveillance is clarified unambiguously (WP 89, par. 22). The data subject must be able to estimate which area is captured by a camera so that he or she is able to avoid surveillance or adapt his or her behaviour if necessary.

#### 7.1.2 Content of the first layer

114. The first layer information (warning sign) should generally convey the most important information, e.g. the details of the purposes of processing, the identity of controller and the existence of the rights of the data subject, together with information on the greatest impacts of the processing.<sup>20</sup> This can include for example the legitimate interests pursued by the controller (or by a third party) and contact details of the data protection officer (if applicable). It also has to refer to the more detailed second layer of information and where and how to find it.
115. In addition the sign should also contain any information that could surprise the data subject (WP260, par. 38). That could for example be transmissions to third parties, particularly if they are located

---

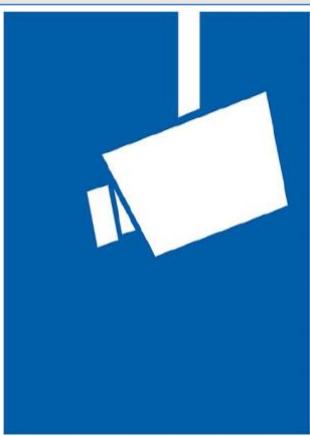
<sup>18</sup> Specific requirements in national legislation might apply.

<sup>19</sup> See WP89, Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance by Article 29 Working Party).

<sup>20</sup> See WP260, par. 38.

outside the EU, and the storage period. If this information is not indicated, the data subject should be able to trust that there is solely a live monitoring (without any data recording or transmission to third parties).

Example (non-binding suggestion):



Identity of the controller and, where applicable, of the controller's representative:

Contact details, including of the data protection officer (where applicable):

Information on the processing that has the most impact on the data subject (e.g. retention period or live monitoring, publication or transmission of video footage to third parties):

Purpose(s) of the video surveillance:



Further information is available:  
• via notice  
• at our reception/ customer information/ register  
• via internet (URL)...

**Data subjects rights:** As a data subject you have several rights to exercise, in particular the right to request from the controller access to or erasure of your personal data.

For details on this video surveillance including your rights, see the full information provided by the controller through the options presented on the left.

116.

## 7.2 Second layer information

117. The second layer information must also be made available at a place easily accessible to the data subject, for example as a complete information sheet available at a central location (e.g. information desk, reception or cashier) or displayed on an easy accessible poster. As mentioned above, the first layer warning sign has to refer clearly to the second layer information. In addition, it is best if the first layer information refers to a digital source (e.g. QR-code or a website address) of the second layer. However, the information should also be easily available non-digitally. It should be possible to access the second layer information without entering the surveyed area, especially if the information is provided digitally (this can be achieved for example by a link). Other appropriate means could be a phone number that can be called. However the information is provided, it must contain all that is mandatory under Article 13 GDPR.
118. In addition to these options, and also to make them more effective, the EDPB promotes the use of technological means to provide information to data subjects. This may include for instance; geolocating cameras and including information in mapping apps or websites so that individuals can easily, on the one hand, identify and specify the video sources related to the exercise of their rights, and on the other hand, obtain more detailed information on the processing operation.

**Example:** A shop owner is monitoring his shop. To comply with Article 13 it is sufficient to place a warning sign at an easy visible point at the entrance of his shop, which contains the first layer information. In addition, he has to provide an information sheet containing the second layer information at the cashier or any other central and easy accessible location in his shop.

119.

## 8 STORAGE PERIODS AND OBLIGATION TO ERASURE

120. Personal data may not be stored longer than what is necessary for the purposes for which the personal data is processed (Article 5 (1) (c) and (e) GDPR). In some Member States, there may be specific provisions for storage periods with regards to video surveillance in accordance with Article 6 (2) GDPR.
121. Whether the personal data is necessary to store or not should be controlled within a narrow timeline. In general, legitimate purposes for video surveillance are often property protection or preservation of evidence. Usually damages that occurred can be recognized within one or two days. To facilitate the demonstration of compliance with the data protection framework it is in the controller's interest to make organisational arrangements in advance (e. g. nominate, if necessary, a representative for screening and securing video material). Taking into consideration the principles of Article 5 (1) (c) and (e) GDPR, namely data minimization and storage limitation, the personal data should in most cases (e.g. for the purpose of detecting vandalism) be erased, ideally automatically, after a few days. The longer the storage period set (especially when beyond 72 hours), the more argumentation for the legitimacy of the purpose and the necessity of storage has to be provided. If the controller uses video surveillance not only for monitoring its premises but also intends to store the data, the controller must assure that the storage is actually necessary in order to achieve the purpose. If so, the storage period needs to be clearly defined and individually set for each particular purpose. It is the controller's responsibility to define the retention period in accordance with the principles of necessity and proportionality and to demonstrate compliance with the provisions of the GDPR.

Example: An owner of a small shop would normally take notice of any vandalism the same day. In consequence, a regular storage period of 24 hours is sufficient. Closed weekends or longer holidays might however be reasons for a longer storage period. If a damage is detected he may also need to store the video footage a longer period in order to take legal action against the offender.

- 122.

## 9 TECHNICAL AND ORGANISATIONAL MEASURES

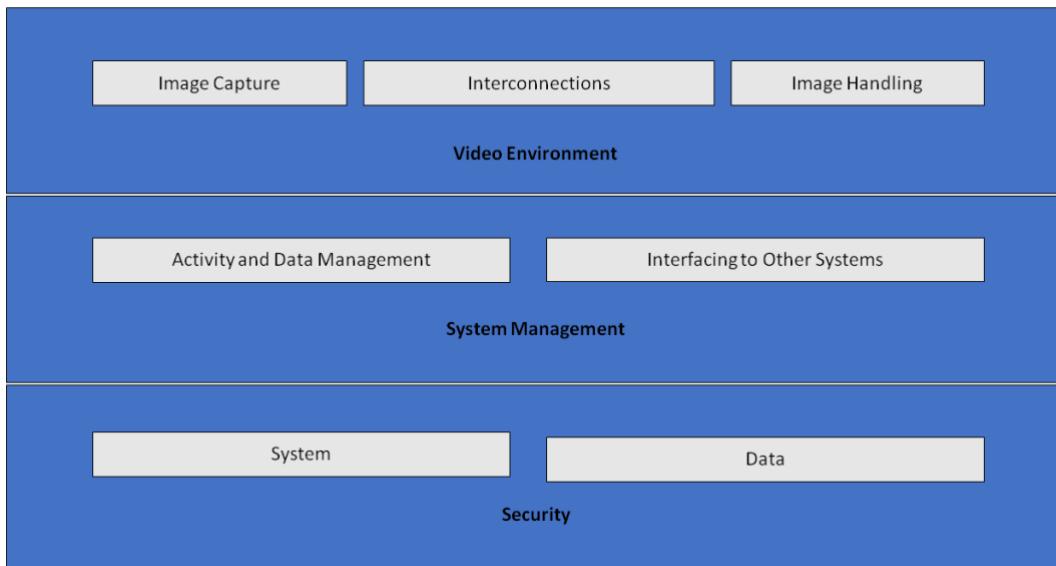
123. As stated in Article 32 (1) GDPR, processing of personal data during video surveillance must not only be legally permissible but controllers and processors must also adequately secure it. Implemented **organizational and technical measures** must be **proportional to the risks to rights and freedoms of natural persons**, resulting from accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to video surveillance data. According to Article 24 and 25 GDPR, controllers need to implement technical and organisational measures also in order to safeguard all data-protection principles during processing, and to establish means for data subjects to exercise their rights as defined in Articles 15-22 GDPR. Data controllers should adopt internal framework and policies that ensure this implementation both at the time of the determination of the means for processing and at the time of the processing itself, including the performance of data protection impact assessments when needed.

## 9.1 Overview of video surveillance system

124. A video surveillance system (VSS)<sup>21</sup> consists of analogue and digital devices as well as software for the purpose of capturing images of a scene, handling the images and displaying them to an operator. Its components are grouped into the following categories:
- Video environment: image capture, interconnections and image handling:
    - the purpose of image capture is the generation of an image of the real world in such format that it can be used by the rest of the system,
    - interconnections describe all transmission of data within the video environment, i.e. connections and communications. Examples of connections are cables, digital networks, and wireless transmissions. Communications describe all video and control data signals, which could be digital or analogue,
    - image handling includes analysis, storage and presentation of an image or a sequence of images.
  - From the system management perspective, a VSS has the following logical functions:
    - data management and activity management, which includes handling operator commands and system generated activities (alarm procedures, alerting operators),
    - interfaces to other systems might include connection to other security (access control, fire alarm) and non-security systems (building management systems, automatic license plate recognition).
  - VSS security consists of system and data confidentiality, integrity and availability:
    - system security includes physical security of all system components and control of access to the VSS,
    - data security includes prevention of loss or manipulation of data.

---

<sup>21</sup> GDPR does not provide a definition for it, a technical description can for example be found in EN 62676-1-1:2014 Video surveillance systems for use in security applications – Part 1-1: Video system requirements.



125.

*Figure 1- video surveillance system*

## 9.2 Data protection by design and by default

- 126. As stated in Article 25 GDPR, controllers need to implement appropriate data protection technical and organisational measures as soon as they plan for video surveillance – before they start the collection and processing of video footage. These principles emphasize the need for built-in privacy enhancing technologies, default settings that minimise the data processing, and the provision of the necessary tools that enable the highest possible protection of personal data<sup>22</sup>.
- 127. Controllers should build data protection and privacy safeguards not only into the design specifications of the technology but also into organisational practices. When it comes to organisational practices, the controller should adopt an appropriate management framework, establish and enforce policies and procedures related to video surveillance. From the technical point of view, system specification and design should include requirements for processing personal data in accordance with principles stated in Article 5 GDPR (lawfulness of processing, purpose and data limitation, data minimisation by default in the sense of Article 25 (2) GDPR, integrity and confidentiality, accountability etc.). In case a controller plans to acquire a commercial video surveillance system, the controller needs to include these requirements in the purchase specification. The controller needs to ensure compliance with these requirements applying them to all components of the system and to all data processed by it, during their entire lifecycle.

## 9.3 Concrete examples of relevant measures

- 128. Most of the measures that can be used to secure video surveillance, especially when digital equipment and software are used, will not differ from those used in other IT systems. However, regardless of the solution selected, the controller must adequately protect all components of a video surveillance system and data under all stages, i.e. during storage (data at rest), transmission (data in transit) and

---

<sup>22</sup> WP 168, Opinion on the "The Future of Privacy", joint contribution by the Article 29 Data Protection Working Party and the Working Party on Police and Justice to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data (adopted on 01 December 2009).

processing (data in use). For this, it is necessary that controllers and processors combine organisational and technical measures.

129. When selecting technical solutions, the controller should consider privacy-friendly technologies also because they enhance security. Examples of such technologies are systems that allow masking or scrambling areas that are not relevant for the surveillance, or the editing out of images of third persons, when providing video footage to data subjects.<sup>23</sup> On the other hand, the selected solutions should not provide functions that are not necessary (e.g., unlimited movement of cameras, zoom capability, radio transmission, analysis and audio recordings). Functions provided, but not necessary, must be deactivated.
130. There is a lot of literature available on this subject, including international standards and technical specifications on the physical security of multimedia systems<sup>24</sup>, and the security of general IT systems<sup>25</sup>. Therefore, this section provides only a high-level overview of this topic.

### 9.3.1 Organisational measures

131. Apart from a potential DPIA needed (see *Section 10*), controllers should consider the following topics when they create their own video surveillance policies and procedures:

- Who is responsible for management and operation of the video surveillance system.
- Purpose and scope of the video surveillance project.
- Appropriate and prohibited use (where and when video surveillance is allowed and where and when it is not; e.g. use of hidden cameras and audio in addition to video recording)<sup>26</sup>.
- Transparency measures as referred to in *Section 7 (Transparency and information obligations)*.
- How video is recorded and for what duration, including archival storage of video recordings related to security incidents.
- Who must undergo relevant training and when.
- Who has access to video recordings and for what purposes.
- Operational procedures (e.g. by whom and from where video surveillance is monitored, what to do in case of a data breach incident).
- What procedures external parties need to follow in order to request video recordings, and procedures for denying or granting such requests.
- Procedures for VSS procurement, installation and maintenance.
- Incident management and recovery procedures.

### 9.3.2 Technical measures

132. **System security** means **physical security** of all system components, and system integrity i.e. **protection against and resilience under intentional and unintentional interference with its normal operations** and **access control**. Data security means **confidentiality** (data is accessible only to those who are granted access), **integrity** (prevention against data loss or manipulation) and **availability** (data can be accessed when it is required).

---

<sup>23</sup> The use of such technologies may even be mandatory in some cases in order to comply with Article 5 (1) (c). In any case they can serve as best practice examples.

<sup>24</sup> IEC TS 62045 — Multimedia security - Guideline for privacy protection of equipment and systems in and out of use.

<sup>25</sup> ISO/IEC 27000 — Information security management systems series.

<sup>26</sup> This may depend on national laws and sector regulations.

133. **Physical security** is a vital part of data protection and the first line of defence, because it protect VSS equipment from theft, vandalism, natural disaster, manmade catastrophes and accidental damage (e.g. from electrical surges, extreme temperatures and spilled coffee). In case of an analogue based systems, physical security plays the main role in their protection.
134. **System and data security**, i.e. protection against intentional and unintentional interference with its normal operations may include:
- Protection of the entire VSS infrastructure (including remote cameras, cabling and power supply) against physical tampering and theft.
  - Protection of footage transmission with communication channels secure against interception
  - Data encryption.
  - Use of hardware and software based solutions such as firewalls, antivirus or intrusion detection systems against cyber attacks.
  - Detection of failures of components, software and interconnections.
  - Means to restore availability and access to the system in the event of a physical or technical incident.
135. **Access control** ensures that only authorized people can access the system and data, while others are prevented from doing it. Measures that support physical and logical access control include:
- Ensuring that all premises where monitoring by video surveillance is done and where video footage is stored are secured against unsupervised access by third parties.
  - Positioning monitors in such a way (especially when they are in open areas, like a reception) so that only authorized operators can view them.
  - Procedures for granting, changing and revoking physical and logical access are defined and enforced.
  - Methods and means of user authentication and authorization including e.g. passwords length and change frequency are implemented.
  - User performed actions (both to the system and data) are recorded and regularly reviewed.
  - Monitoring and detection of access failures is done continuously and identified weaknesses are addressed as soon as possible.

## 10 DATA PROTECTION IMPACT ASSESSMENT

136. According to Article 35 (1) GDPR controllers are required to conduct data protection impact assessments (DPIA) when a type of data processing is likely to result in a high risk to the rights and freedoms of natural persons. Article 35 (3) (c) GDPR stipulates that controllers are required to carry out data protection impact assessments if the processing constitutes a systematic monitoring of a publicly accessible area on a large scale. Moreover, according to Article 35 (3) (b) GDPR a data protection impact assessment is also required when the controller intends to process special categories of data on a large scale.
137. The Guidelines on Data Protection Impact Assessment<sup>27</sup> provide further advice, and more detailed examples relevant to video surveillance (e.g. concerning the “use of a camera system to monitor driving behaviour on highways”). Article 35 (4) GDPR requires that each supervisory authority publish a list of the kind of processing operations that are subject to mandatory DPIA within their country. These lists can usually be found on the authorities’ websites. Given the typical purposes of video surveillance (protection of people and property, detection, prevention and control of offences, collection of evidence and biometric identification of suspects), it is reasonable to assume that many cases of video surveillance will require a DPIA. Therefore, data controllers should carefully consult these documents in order to determine whether such an assessment is required and conduct it if necessary. The outcome of the performed DPIA should determine the controller’s choice of implemented data protection measures.
138. It is also important to note that if the results of the DPIA indicate that processing would result in a high risk despite security measures planned by the controller, then it will be necessary to consult the relevant supervisory authority prior to the processing. Details on prior consultations can be found in Article 36.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

---

<sup>27</sup> WP248 rev.01, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. - endorsed by the EDPB

# Guidelines



**Guidelines 4/2019 on Article 25**

**Data Protection by Design and by Default**

**Version 2.0**

**Adopted on 20 October 2020**

## Version history

Version 1.0	13 November 2019	Adoption of the Guidelines for public consultation
Version 2.0	20 October 2020	Adoption of the Guidelines by the EDPB after public consultation

## Table of contents

1	Scope .....	5
2	Analysis of Article 25(1) and (2) of the GDPR.....	5
2.1	Article 25(1) of the GDPR: Data protection by design.....	6
2.1.1	Controller's obligation to implement appropriate technical and organisational measures and necessary safeguards into the processing .....	6
2.1.2	Designed to implement the data protection principles in an effective manner and protecting data subjects' rights and freedoms .....	6
2.1.3	Elements to take into account .....	7
2.1.4	Time aspect .....	10
2.2	Article 25(2): Data protection by default .....	11
2.2.1	By default, only personal data which are necessary for each specific purpose of the processing are processed .....	11
2.2.2	Dimensions of the data minimisation obligation .....	12
3	Implementing data protection principles in the processing of personal data using data protection by design and by default .....	14
3.1	Transparency .....	15
3.2	Lawfulness .....	16
3.3	Fairness.....	17
3.4	Purpose Limitation .....	19
3.5	Data Minimisation .....	21
3.6	Accuracy .....	23
3.7	Storage limitation .....	25
3.8	Integrity and confidentiality.....	26
3.9	Accountability.....	28
4	Article 25(3) Certification .....	28
5	Enforcement of Article 25 and consequences .....	29
6	Recommendations .....	29

# The European Data Protection Board

Having regard to Article 70 (1e) 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,

## HAS ADOPTED THE FOLLOWING GUIDELINES

### Executive summary

In an increasingly digital world, adherence to Data Protection by Design and by Default requirements plays a crucial part in promoting privacy and data protection in society. It is therefore essential that controllers take this responsibility seriously and implement the GDPR obligations when designing processing operations.

These Guidelines give general guidance on the obligation of Data Protection by Design and by Default (henceforth “DPbDD”) set forth in Article 25 in the GDPR. DPbDD is an obligation for all controllers, irrespective of size and varying complexity of processing. To be able to implement the requirements of DPbDD, it is crucial that the controller understands the data protection principles and the data subject’s rights and freedoms.

The core obligation is the implementation of *appropriate measures* and necessary safeguards that provide *effective implementation* of the *data protection principles* and, consequentially, *data subjects’ rights and freedoms by design and by default*. Article 25 prescribes both design and default elements that should be taken into account. Those elements, will be further elaborated in these Guidelines.

Article 25(1) stipulates that controllers should consider DPbDD early on when they plan a new processing operation. Controllers shall implement DPbDD *before* processing, and also *continually* at the time of processing, by regularly reviewing the effectiveness of the chosen measures and safeguards. DPbDD also applies to existing systems that are processing personal data.

The Guidelines also contain guidance on how to effectively implement the data protection principles in Article 5, listing key design and default elements as well as practical cases for illustration. The controller should consider the appropriateness of the suggested measures in the context of the particular processing in question.

The EDPB provides recommendations on how controllers, processors and producers can cooperate to achieve DPbDD. It encourages the controllers in industry, processors, and producers to use DPbDD as a means to achieve a competitive advantage when marketing their products towards controllers and data subjects. It also encourages all controllers to make use of certifications and codes of conduct.

## 1 SCOPE

1. The Guidelines focus on controllers' implementation of DPbDD based on the obligation in Article 25 of the GDPR.<sup>1</sup> Other actors, such as processors and producers of products, services and applications (henceforth "producers"), who are not directly addressed in Article 25, may also find these Guidelines useful in creating GDPR compliant products and services that enable controllers to fulfil their data protection obligations.<sup>2</sup> Recital 78 of the GDPR adds that DPbDD should be taken into consideration in the context of public tenders. Despite all controllers having the duty to integrate DPbDD into their processing activities, this provision fosters the adoption of the data protection principles, where public administrations should lead by example. The controller is responsible for the fulfilment of the DPbDD obligations for the processing carried out by their processors and sub-processors, they should therefore take this into account when contracting with these parties.
2. The requirement described in Article 25 is for controllers to have data protection designed into the processing of personal data and as a default setting and this applies throughout the processing lifecycle. DPbDD is also a requirement for processing systems pre-existing before the GDPR entered into force. Controllers must have the processing consistently updated in line with the GDPR. For more information on how to maintain an existing system in line with DPbDD, see subchapter 2.1.4 of these Guidelines. The core of the provision is to ensure *appropriate* and *effective* data protection both by *design* and by *default*, which means that controllers should be able to demonstrate that they have the appropriate measures and safeguards in the processing to ensure that the data protection principles and the rights and freedoms of data subjects are effective.
3. Chapter 2 of the Guidelines focuses on an interpretation of the requirements set forth by Article 25 and explores the legal obligations introduced by the provision. Examples on how to apply DPbDD in the context of specific data protection principles are provided in Chapter 3.
4. The Guidelines address the possibility to establish a certification mechanism to demonstrate compliance with Article 25 in Chapter 4, as well as how the Article may be enforced by supervisory authorities in Chapter 5. Finally, the Guidelines provide stakeholders with further recommendations on how to successfully implement DPbDD. The EDPB recognizes the challenges for small and medium enterprises (henceforth "SMEs") to fully comply with the obligations of DPbDD, and provides additional recommendations specifically to SMEs in Chapter 6.

## 2 ANALYSIS OF ARTICLE 25(1) AND (2) DATA PROTECTION BY DESIGN AND BY DEFAULT

5. The aim of this Chapter is to explore and provide guidance on the requirements to data protection by design in Article 25(1) and to data protection by default in Article 25(2) respectively. Data protection

---

<sup>1</sup> The interpretations provided herein equally apply to Article 20 of Directive (EU) 2016/680, and Article 27 of Regulation 2018/1725.

<sup>2</sup> Recital 78 GDPR clearly states this need: "*When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the "state of the art", to make sure that controllers and processors are able to fulfil their data protection obligations*".

by design and data protection by default are complementary concepts, which mutually reinforce each other. Data subjects will benefit more from data protection by default if data protection by design is concurrently implemented – and vice versa.

6. DPbDD is a requirement for all controllers, including small businesses and multinational companies alike. That being the case, the complexity of implementing DPbDD may vary based on the individual processing operation. Regardless of the size however, in all cases, positive benefits for controller and data subject can be achieved by implementing DPbDD.

## 2.1 Article 25(1): Data protection by design

### 2.1.1 Controller's obligation to implement appropriate technical and organisational measures and necessary safeguards into the processing

7. In line with Article 25(1) the controller shall implement *appropriate* technical and organisational *measures* which are designed to implement the data protection principles and to integrate the *necessary safeguards* into the processing in order to meet the requirements and protect the rights and freedoms of data subjects. Both appropriate measures and necessary safeguards are meant to serve the same purpose of protecting the rights of data subjects and ensuring that the protection of their personal data is built into the processing.
  8. *Technical and organizational measures* and necessary *safeguards* can be understood in a broad sense as any method or means that a controller may employ in the processing. Being *appropriate* means that the measures and necessary safeguards should be suited to achieve the intended purpose, i.e. they must implement the data protection principles *effectively*<sup>3</sup>. The requirement to appropriateness is thus closely related to the requirement of effectiveness.
  9. A technical or organisational measure and safeguard can be anything from the use of advanced technical solutions to the basic training of personnel. Examples that may be suitable, depending on the context and risks associated with the processing in question, includes pseudonymization of personal data<sup>4</sup>; storing personal data available in a structured, commonly machine readable format; enabling data subjects to intervene in the processing; providing information about the storage of personal data; having malware detection systems; training employees about basic “cyber hygiene”; establishing privacy and information security management systems, obligating processors contractually to implement specific data minimisation practices, etc.
  10. Standards, best practices and codes of conduct that are recognized by associations and other bodies representing categories of controllers can be helpful in determining appropriate measures. However, the controller must verify the appropriateness of the measures for the particular processing in question.
- ### 2.1.2 Designed to implement the data protection principles in an effective manner and protecting data subjects' rights and freedoms
11. The *data protection principles* are in Article 5 (henceforth “the principles”), the *data subjects' rights and freedoms* are the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data, whose protection is named in Article 1(2) as the objective of the

---

<sup>3</sup> “Effectiveness” is addressed below in subchapter 2.1.2.

<sup>4</sup> Defined in Article 4(5) GDPR.

GDPR (henceforth “the rights”)<sup>5</sup>. Their precise formulation can be found in the EU Charter of Fundamental Rights. It is essential for the controller to have an understanding of the meaning of *the principles* and *the rights* as the basis for the protection offered by the GDPR, specifically by the DPbDD obligation.

12. When implementing the appropriate technical and organisational measures, it is with respect to the effective implementation of each of the aforementioned principles and the ensuing protection of rights that the measures and safeguards should be *designed*.

#### **Addressing effectiveness**

13. Effectiveness is at the heart of the concept of data protection by design. The requirement to implement the principles in an effective manner means that controllers must implement the necessary measures and safeguards to protect these principles, in order to secure the rights of data subjects. Each implemented measure should produce the intended results for the processing foreseen by the controller. This observation has two consequences.
  14. First, it means that Article 25 does not require the implementation of any specific technical and organizational measures, rather that the chosen measures and safeguards should be specific to the implementation of data protection principles into the particular processing in question. In doing so, the measures and safeguards should be designed to be robust and the controller should be able to implement further measures in order to scale to any increase in risk<sup>6</sup>. Whether or not measures are effective will therefore depend on the context of the processing in question and an assessment of certain elements that should be taken into account when determining the means of processing. The aforementioned elements will be addressed below in subchapter 2.1.3.
  15. Second, controllers should be able to demonstrate that the principles have been maintained.
  16. The implemented measures and safeguards should achieve the desired effect in terms of data protection, and the controller should have documentation of the implemented technical and organizational measures.<sup>7</sup> To do so, the controller may determine appropriate key performance indicators (KPI) to demonstrate the effectiveness. A KPI is a measurable value chosen by the controller that demonstrates how effectively the controller achieves their data protection objective. KPIs may be *quantitative*, such as the percentage of false positives or false negatives, reduction of complaints, reduction of response time when data subjects exercise their rights; or *qualitative*, such as evaluations of performance, use of grading scales, or expert assessments. Alternatively to KPIs, controllers may be able to demonstrate the effective implementation of the principles by providing the rationale behind their assessment of the effectiveness of the chosen measures and safeguards.

#### **2.1.3 Elements to take into account**

17. Article 25 (1) lists elements that the controller has to take into account when determining the measures of a specific processing operation. In the following, we will provide guidance on how to apply

---

<sup>5</sup> See Recital 4 of the GDPR.

<sup>6</sup> “Fundamental principles applicable to the controllers (i.e. legitimacy, data minimisation, purpose limitation, transparency, data integrity, data accuracy) should remain the same, whatever the processing and the risks for the data subjects. However, due regard to the nature and scope of such processing have always been an integral part of the application of those principles, so that they are inherently scalable.” Article 29 Working Party. “Statement on the role of a risk-based approach in data protection legal frameworks”. WP 218, 30 May 2014, p. 3. [ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218\\_en.pdf](http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf)

<sup>7</sup> See Recitals 74 and 78.

these elements in the design process, which includes design of the default settings. These elements all contribute to determine whether a measure is appropriate to effectively implement the principles. Thus, each of these elements is not a goal in and of themselves, but are factors to be considered together to reach the objective.

#### *2.1.3.1 “state of the art”*

18. The concept of “state of the art” is present in various EU acquis, e.g. environmental protection and product safety. In the GDPR, reference to the “state of the art”<sup>8</sup> is made not only in Article 32, for security measures,<sup>910</sup> but also in Article 25, thus extending this benchmark to all technical and organisational measures embedded in the processing.
19. In the context of Article 25, the reference to “state of the art” imposes an obligation on controllers, when determining the appropriate technical and organisational measures, **to take account of the current progress in technology** that is available in the market. The requirement is for controllers to have knowledge of, and stay up to date on technological advances; how technology can present data protection risks or opportunities to the processing operation; and how to implement and update the measures and safeguards that *secure effective implementation* of the principles and rights of data subjects taking into account the evolving technological landscape.
20. The “state of the art” is a dynamic concept that cannot be statically defined at a fixed point in time, but should be assessed *continuously* in the context of technological progress. In the face of technological advancements, a controller could find that a measure that once provided an adequate level of protection no longer does. Neglecting to keep up to date with technological changes could therefore result in a lack of compliance with Article 25.
21. The “state of the art” criterion does not only apply to technological measures, but also to organisational ones. Lack of appropriate organisational measures can lower or even completely undermine the effectiveness of a chosen technology. Examples of organisational measures can be adoption of internal policies; up-to date training on technology, security and data protection; and IT security governance and management policies.
22. Existing and recognized frameworks, standards, certifications, codes of conduct, etc. in different fields may play a role in indicating the current “state of the art” within the given field of use. Where such standards exist and provide a high level of protection for the data subject in compliance with – or go beyond – legal requirements, controllers should take them into account in the design and implementation of data protection measures.

#### *2.1.3.2 “cost of implementation”*

23. The controller may take the cost of implementation into account when choosing and applying appropriate technical and organisational measures and necessary safeguards that effectively

---

<sup>8</sup> See German Federal Constitutional Court’s “Kalkar” decision in 1978:  
<https://germanlawarchive.iuscomp.org/?p=67> may provide the foundation for a methodology for an objective definition of the concept. On that basis, the “state of the art” technology level would be identified between the “existing scientific knowledge and research” technology level and the more established “generally accepted rules of technology”. The “state of the art” can hence be identified as the technology level of a service or technology or product that exists in the market and is most effective in achieving the objectives identified.

<sup>9</sup> <https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security>

<sup>10</sup> [www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/](http://www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/)

implement the principles in order to protect the rights of data subjects. The cost refers to resources in general, including time and human resources.

24. The cost element does not require the controller to spend a disproportionate amount of resources when alternative, less resource demanding, yet effective measures exist. However, the cost of implementation is a factor to be considered to implement data protection by design rather than a ground to not implement it.
25. Thus, the chosen measures shall ensure that the processing activity foreseen by the controller does not process personal data in violation of the principles, independent of cost. Controllers should be able to manage the overall costs to be able to effectively implement all of the principles and, consequentially, protect the rights.

#### *2.1.3.3 “nature, scope, context and purpose of processing”*

26. Controllers must take into consideration the nature, scope, context and purpose of processing when determining needed measures.
27. These factors should be interpreted consistently with their role in other provisions of the GDPR, such as Articles 24, 32 and 35, with the aim of designing data protection principles into the processing.
28. In short, the concept of **nature** can be understood as the inherent<sup>11</sup> characteristics of the processing. The **scope** refers to the size and range of the processing. The **context** relates to the circumstances of the processing, which may influence the expectations of the data subject, while the **purpose** pertains to the aims of the processing.

#### *2.1.3.4 “risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing”*

29. The GDPR adopts a coherent risk based approach in many of its provisions, in Articles 24, 25, 32 and 35, with a view to identifying appropriate technical and organisational measures to protect individuals, their personal data and complying with the requirements of the GDPR. The assets to protect are always the same (the individuals, via the protection of their personal data), against the same risks (to individuals' rights), taking into account the same conditions (nature, scope, context and purposes of processing).
30. When performing the risk analysis for compliance with Articles 25, the controller has to identify the risks to the rights of data subjects that a violation of the principles presents, and determine their likelihood and severity in order to implement measures to effectively mitigate the identified risks. A systematic and thorough evaluation of the processing is crucial when doing risk assessments. For example, a controller assesses the particular risks associated with a lack of freely given consent, which constitutes a violation of the lawfulness principle, in the course of the processing of personal data of children and young people under 18 as a vulnerable group, in a case where no other legal ground exists, and implements appropriate measures to address and effectively mitigate the identified risks associated with this group of data subjects.

---

<sup>11</sup> Examples are special categories personal data, automatic decision-making, skewed power relations, unpredictable processing, difficulties for the data subject to exercise the rights, etc.

31. The “EDPB Guidelines on Data Protection Impact Assessment (DPIA)”,<sup>12</sup> which focus on determining whether a processing operation is likely to result in a high risk to the data subject or not, also provide guidance on how to assess data protection risks and how to carry out a data protection risk assessment. These Guidelines may also be useful during the risk assessment in all the articles mentioned above, including Article 25.
32. The risk based approach does not exclude the use of baselines, best practices and standards. These might provide a useful toolbox for controllers to tackle similar risks in similar situations (nature, scope, context and purpose of processing). Nevertheless, the obligation in Article 25 (as well as Articles 24, 32 and 35(7)(c)) to take into account “*risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing*” remains. Therefore, controllers, although supported by such tools, must always carry out a data protection risk assessment on a case by case basis for the processing activity at hand and verify the effectiveness of the appropriate measures and safeguards proposed. A DPIA, or an update to an existing DPIA, may then additionally be required.

#### 2.1.4 Time aspect

##### 2.1.4.1 At the time of the determination of the means for processing

33. Data protection by design shall be implemented “*at the time of determination of the means for processing*”.
34. The “*means for processing*” range from the general to the detailed design elements of the processing, including the architecture, procedures, protocols, layout and appearance.
35. The “*time of determination of the means for processing*” refers to the period of time when the controller is deciding how the processing will be conducted and the manner in which the processing will occur and the mechanisms which will be used to conduct such processing. It’s in the process of making such decisions that the controller must assess the appropriate measures and safeguards to effectively implement the principles and rights of data subjects into the processing, and take into account elements such as the state of the art, cost of implementation, nature, scope, context and purpose, and risks. This includes the time of procuring and implementing data processing software, hardware, and services.
36. Early consideration of DPbDD is crucial for a successful implementation of the principles and protection of the rights of the data subjects. Moreover, from a cost-benefit perspective, it is also in controllers’ interest to take DPbDD into account sooner rather than later, as it could be challenging and costly to make later changes to plans that have already been made and processing operations that have already been designed.

##### 2.1.4.2 At the time of the processing itself (maintenance and review of data protection requirements)

37. Once the processing has started the controller has a continued obligation to maintain DPbDD, i.e. the continued effective implementation of the principles in order to protect the rights, staying up to date on the state of the art, reassessing the level of risk, etc. The nature, scope and context of processing operations, as well as the risk may change over the course of processing, which means that the

---

<sup>12</sup> Article 29 Working Party “Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679”. WP 248 rev.01, 4 October 2017. [ec.europa.eu/newsroom/document.cfm?doc\\_id=47711](http://ec.europa.eu/newsroom/document.cfm?doc_id=47711) - endorsed by the EDPB.

controller must re-evaluate their processing operations through regular reviews and assessments of the effectiveness of their chosen measures and safeguards.

38. The obligation to maintain, review and update, as necessary, the processing operation also applies to pre-existing systems. This means that legacy systems designed before the GDPR entered into force are required to undergo reviews and maintenance to ensure the implementation of measures and safeguards that implement the principles and rights of data subjects in an effective manner, as outlined in these Guidelines.
39. This obligation also extends to any processing carried out by means of data processors. Processors' operations should be regularly reviewed and assessed by the controllers to ensure that they enable continuous compliance with the principles and allow the data controller to fulfil its obligations in this respect.

## 2.2 Article 25(2): Data protection by default

### 2.2.1 By default, only personal data which are necessary for each specific purpose of the processing are processed

40. A “default”, as commonly defined in computer science, refers to the pre-existing or preselected value of a configurable setting that is assigned to a software application, computer program or device. Such settings are also called “presets” or “factory presets”, especially for electronic devices.
41. Hence, the term “by default” when processing personal data, refers to making choices regarding configuration values or processing options that are set or prescribed in a processing system, such as a software application, service or device, or a manual processing procedure that affect the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.
42. The controller should choose and be accountable for implementing default processing settings and options in a way that only processing that is strictly necessary to achieve the set, lawful purpose is carried out by default. Here, controllers should rely on their assessment of the necessity of the processing with regards to the legal grounds of Article 6(1). This means that by default, the controller shall not collect more data than is necessary, they shall not process the data collected more than is necessary for their purposes, nor shall they store the data for longer than necessary. The basic requirement is that data protection is built into the processing by default.
43. The controller is required to predetermine for which specified, explicit and legitimate purposes the personal data is collected and processed.<sup>13</sup> The measures must by default be appropriate to ensure that only personal data which are necessary for each specific purpose of processing are being processed. The EDPS “Guidelines to assess necessity and proportionality of measures that limit the

---

<sup>13</sup> Art. 5(1)(b), (c), (d), (e) GDPR.

right to data protection of personal data” can be useful also to decide which data is necessary to process in order to achieve a specific purpose.<sup>14 15 16</sup>

44. If the controller uses third party software or off-the-shelf software, the controller should carry out a risk assessment of the product and make sure that functions that do not have a legal basis or are not compatible with the intended purposes of processing are switched off.
45. The same considerations apply to organisational measures supporting processing operations. They should be designed to process, at the outset, only the minimum amount of personal data necessary for the specific operations. This should be particularly considered when allocating data access to staff with different roles and different access needs.
46. Appropriate “technical and organisational measures” in the context of data protection by default is thus understood in the same way as discussed above in subchapter 2.1.1, but applied specifically to implementing the principle of data minimisation.
47. The aforementioned obligation to only process personal data which are necessary for each specific purpose applies to the following elements.

## 2.2.2 Dimensions of the data minimisation obligation

48. Article 25 (2) lists the dimensions of the data minimisation obligation for default processing, by stating that the obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

### 2.2.2.1 *“amount of personal data collected”*

49. Controllers should consider both the volume of personal data, as well as the types, categories and level of detail of personal data required for the processing purposes. Their design choices should take into account the increased risks to the principles of integrity and confidentiality, data minimisation and storage limitation when collecting large amounts of detailed personal data, and compare it to the reduction in risks when collecting smaller amounts and/or less detailed information about data subjects. In any case, the default setting shall not include collection of personal data that is not necessary for the specific processing purpose. In other words, if certain categories of personal data are unnecessary or if detailed data isn’t needed because less granular data is sufficient, then any surplus personal data shall not be collected.
50. The same default requirements apply to services independent of what platform or device in use, only the necessary personal data for the given purpose can be collected.

---

<sup>14</sup> EDPS. “Guidelines on assessing the necessity and proportionality of measures that limit the right to data protection”. 25 February 2019. [edps.europa.eu/sites/edp/files/publication/19-02-25\\_proportionality\\_guidelines\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf)

<sup>15</sup> See also EDPS. “Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit” [https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit\\_en](https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en)

<sup>16</sup> For more information on necessity, see Article 29 Working Party. “Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC”. WP 217, 9 April 2014. [ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217\\_en.pdf](http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf)

#### *2.2.2.2 “the extent of their processing”*

51. Processing<sup>17</sup> operations performed on personal data shall be limited to what is necessary. Many processing operations may contribute to a processing purpose. Nevertheless, the fact that certain personal data is necessary to fulfil a purpose does not mean that all types of, and frequencies of, processing operations may be carried out on the data. Controllers should also be careful not to extend the boundaries of “compatible purposes” of Article 6(4), and have in mind what processing will be within the reasonable expectations of data subjects.

#### *2.2.2.3 “the period of their storage”*

52. Personal data collected shall not be stored if it is not necessary for the purpose of the processing and there is no other compatible purpose and legal ground according to Article 6(4). Any retention should be objectively justifiable as necessary by the data controller in accordance with the accountability principle.
53. The controller shall limit the retention period to what is necessary for the purpose. If personal data is no longer necessary for the purpose of the processing, then it shall by default be deleted or anonymized. The length of the period of retention will therefore depend on the purpose of the processing in question. This obligation is directly related to the principle of storage limitation in Article 5(1)(e), and shall be implemented by default, i.e. the controller should have systematic procedures for data deletion or anonymization embedded in the processing.
54. Anonymization<sup>18</sup> of personal data is an alternative to deletion, provided that all the relevant contextual elements are taken into account and the likelihood and severity of the risk, including the risk of re-identification, are regularly assessed.<sup>19</sup>

#### *2.2.2.4 “their accessibility”*

55. The controller should limit who has access and which types of access to personal data based on an assessment of necessity, and also make sure that personal data is in fact accessible to those who need it when necessary, for example in critical situations. Access controls should be observed for the whole data flow during the processing.
56. Article 25(2) further states that personal data shall not be made accessible, without the individual’s intervention, to an indefinite number of natural persons. The controller shall by default limit accessibility and give the data subject the possibility to intervene before publishing or otherwise making available personal data about the data subject to an indefinite number of natural persons.
57. Making personal data available to an indefinite number of persons may result in even further dissemination of the data than initially intended. This is particularly relevant in the context of the Internet and search engines. This means that controllers should by default give data subjects an

---

<sup>17</sup> According to Art. 4(2) GDPR, this includes 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.

<sup>18</sup> Article 29 Working Party. “Opinion 05/2014 on Anonymisation Techniques”. WP 216, 10 April 2014. [ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216\\_en.pdf](http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf)

<sup>19</sup> Please see Art. 4(1) GDPR, Recital 26 GDPR, Article 29 Working Party “Opinion 05/2014 on Anonymisation Techniques”. Please also see the subsection on “storage limitation” in section 3 of this document, referring to the need for the controller to ensure the effectiveness of the implemented anonymisation technique(s).

opportunity to intervene before personal data is made available on the open Internet. This is particularly important when it comes to children and vulnerable groups.

58. Depending on the legal grounds for processing, the opportunity to intervene could vary based on the context of the processing. For example, to ask for consent to make the personal data publicly accessible, or to have privacy settings so that data subjects themselves can control public access.
59. Even in the event that personal data is made available publicly with the permission and understanding of a data subject, it does not mean that any other controller with access to the personal data may freely process it themselves for their own purposes – they must have their own legal basis.<sup>20</sup>

### 3 IMPLEMENTING DATA PROTECTION PRINCIPLES IN THE PROCESSING OF PERSONAL DATA USING DATA PROTECTION BY DESIGN AND BY DEFAULT

60. In all stages of design of the processing activities, including procurement, tenders, outsourcing, development, support, maintenance, testing, storage, deletion, etc., the controller should take into account and consider the various elements of DPbDD which will be illustrated by examples in this chapter in the context of implementation of the principles.<sup>21 22 23</sup>
61. Controllers need to implement the principles to achieve DPbDD. These principles include: transparency, lawfulness, fairness, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability. These principles are outlined in Article 5 and Recital 39 of the GDPR. To have a complete understanding of how to implement DPbDD, the importance of understanding the meaning of each of the principles is emphasised.
62. When presenting examples of how to operationalize DPbDD we have made lists of **key DPbDD elements** for each of the principles. The examples, while highlighting the specific data protection principle in question, may overlap with other closely related principles as well. The EDPB underlines that the key elements and the examples presented hereunder are neither exhaustive nor binding, but are meant as guiding elements for each of the principles. Controllers need to assess how to guarantee compliance with the principles in the context of the concrete processing operation in question.
63. While this section focuses on the implementation of the principles, the controller should also implement *appropriate* and *effective* ways to protect data subjects' rights, also according to Chapter III in the GDPR where this is not already mandated by the principles themselves.
64. The accountability principle is overarching: it requires the controller to be responsible choosing the necessary technical and organisational measures.

---

<sup>20</sup> See Case of Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland no. 931/13.

<sup>21</sup> More examples can be found in Norwegian Data Protection Authority. "Software Development with Data Protection by Design and by Default". 28 November 2017. [www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?id=7729](http://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?id=7729)

<sup>22</sup> <https://www.cnil.fr/en/cnil-publishes-gdpr-guide-developers>

<sup>23</sup> [https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno\\_en.pdf](https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf)

### 3.1 Transparency<sup>24</sup>

65. The controller must be clear and open with the data subject about how they will collect, use and share personal data. Transparency is about enabling data subjects to understand, and if necessary, make use of their rights in Articles 15 to 22. The principle is embedded in Articles 12, 13, 14 and 34. Measures and safeguards put in place to support the principle of transparency should also support the implementation of these Articles.
66. Key design and default elements for the principle of transparency may include:
  - ] Clarity – Information shall be in clear and plain language, concise and intelligible.
  - ] Semantics – Communication should have a clear meaning to the audience in question.
  - ] Accessibility - Information shall be easily accessible for the data subject.
  - ] Contextual – Information should be provided at the relevant time and in the appropriate form.
  - ] Relevance – Information should be relevant and applicable to the specific data subject.
  - ] Universal design – Information shall be accessible to all data subjects, include use of machine readable languages to facilitate and automate readability and clarity.
  - ] Comprehensible – Data subjects should have a fair understanding of what they can expect with regards to the processing of their personal data, particularly when the data subjects are children or other vulnerable groups.
  - ] Multi-channel – Information should be provided in different channels and media, not only the textual, to increase the probability for the information to effectively reach the data subject.
  - ] Layered – The information should be layered in a manner that resolves the tension between completeness and understanding, while accounting for data subjects' reasonable expectations.

#### Example<sup>25</sup>

A controller is designing a privacy policy on their website in order to comply with the requirements of transparency. The privacy policy should not contain a lengthy bulk of information that is difficult for the average data subject to penetrate and understand. It shall be written in clear and concise language and make it easy for the user of the website to understand how their personal data is processed. The controller therefore provides information in a layered manner, where the most important points are highlighted. More detailed information is made easily available. Drop-down menus and links to other pages are provided to further explain the various items, and concepts used in the policy. The controller also makes sure that the information is provided in a multi-channel manner, providing video clips to explain the most important points of the written information. Synergy between the various pages is vital to ensure that the layered approach does not heighten confusion, rather reduce it.

The privacy policy should not be difficult for data subjects to access. The privacy policy is thus made available and visible on all web-pages of the site in question, so that the data subject is always only one click away from accessing the information. The information provided is also designed in accordance with the best practices and standards of universal design to make it accessible to all.

<sup>24</sup> Elaboration on how to understand the concept of transparency can be found in Article 29 Working Party. "Guidelines on transparency under Regulation 2016/679". WP 260 rev.01, 11 April 2018.

[ec.europa.eu/newsroom/article29/document.cfm?action=display&doc\\_id=51025](http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025) - endorsed by the EDPB

<sup>25</sup> The French Data Protection Authority has published several examples illustrating best practices in informing users as well as other transparency principles: <https://design.cnil.fr/en/>.

Moreover, necessary information should also be provided in the right context, at the appropriate time. Since the controller carries out many processing operations using the data collected on the website, a general privacy policy on the website alone is not sufficient for the controller to meet the requirements of transparency. The controller therefore designs an information flow, presenting the data subject with relevant information within the appropriate contexts using e.g. informational snippets or pop-ups. For example, when asking the data subject to enter personal data, the controller informs the data subject of how the personal data will be processed and why that personal data is necessary for the processing.

### 3.2 Lawfulness

67. The controller must identify a valid legal basis for the processing of personal data. Measures and safeguards should support the requirement to make sure that the whole processing lifecycle is in line with the relevant legal grounds of processing.
68. Key design and default elements for lawfulness may include:
  - Relevance – The correct legal basis shall be applied to the processing.
  - Differentiation<sup>26</sup> – The legal basis used for each processing activity shall be differentiated.
  - Specified purpose – The appropriate legal basis must be clearly connected to the specific purpose of processing.<sup>27</sup>
  - Necessity – Processing must be necessary and unconditional for the purpose to be lawful.
  - Autonomy – The data subject should be granted the highest degree of autonomy as possible with respect to control over personal data within the frames of the legal basis.
  - Gaining consent – consent must be freely given, specific, informed and unambiguous.<sup>28</sup> Particular consideration should be given to the capacity of children and young people to provide informed consent.
  - Consent withdrawal – Where consent is the legal basis, the processing should facilitate withdrawal of consent. Withdrawal shall be as easy as giving consent. If not, then the consent mechanism of the controller does not comply with the GDPR.<sup>29</sup>
  - Balancing of interests – Where legitimate interests is the legal basis, the controller must carry out a weighted balancing of interest, giving particular consideration to the power imbalance, specifically children under the age of 18 and other vulnerable groups. There shall be measures and safeguards to mitigate the negative impact on the data subjects.
  - Predetermination – The legal basis shall be established before the processing takes place.
  - Cessation – If the legal basis ceases to apply, the processing shall cease accordingly.
  - Adjust – If there is a valid change of legal basis for the processing, the actual processing must be adjusted in accordance with the new legal basis.<sup>30</sup>

<sup>26</sup> EDPB. "Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects". Version 2.0, 8 October 2019.

[edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_guidelines-art\\_6-1-b-adopted\\_after\\_public\\_consultation\\_en.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf)

<sup>27</sup> See section on purpose limitation below.

<sup>28</sup> See Guidelines 05/2020 on consent under Regulation 2016/679. [https://edpb.europa.eu/our-work-tools/our-documents/guidelines-guidelines-052020-consent-under-regulation-2016679\\_en](https://edpb.europa.eu/our-work-tools/our-documents/guidelines-guidelines-052020-consent-under-regulation-2016679_en)

<sup>29</sup> See Guidelines 05/2020 on consent under Regulation 2016/679, p. 24. [https://edpb.europa.eu/our-work-tools/our-documents/guidelines-guidelines-052020-consent-under-regulation-2016679\\_en](https://edpb.europa.eu/our-work-tools/our-documents/guidelines-guidelines-052020-consent-under-regulation-2016679_en)

<sup>30</sup> If the original legal basis is consent, see Guidelines 05/2020 on consent under Regulation 2016/679. [https://edpb.europa.eu/our-work-tools/our-documents/guidelines-guidelines-052020-consent-under-regulation-2016679\\_en](https://edpb.europa.eu/our-work-tools/our-documents/guidelines-guidelines-052020-consent-under-regulation-2016679_en)

- J Allocation of responsibility – Whenever joint controllership is envisaged, the parties must apportion in a clear and transparent way their respective responsibilities vis-à-vis the data subject, and design the measures of the processing in accordance with this allocation.

Example

A bank plans to offer a service to improve efficiency in the management of loan applications. The idea behind the service is that the bank, by requesting permission from the customer, is able to retrieve data about the customer directly from the public tax authorities. This example does not consider processing of personal data from other sources.

Obtaining personal data about the data subject's financial situation is necessary in order to take steps at the request of the data subject prior to entering into a loan contract.<sup>31</sup> However, gathering personal data directly from the tax administration is not considered necessary, because the customer is able to enter into a contract by providing the information from the tax administration him or herself. Although the bank may have a legitimate interest in acquiring the documentation from the tax authorities directly, for example to ensure efficiency in the loan processing, giving banks such direct access to the personal data of applicants presents a risks related to the use or potential misuse of access rights

When implementing the principle of lawfulness, the controller realizes that in this context, they cannot use the "necessary for contract" basis for the part of the processing that involves gathering personal data directly from the tax authorities. The fact that this specific processing presents a risk of the data subject becoming less involved in the processing of their data is also a relevant factor in assessing the lawfulness of the processing itself. The bank concludes that this part of the processing has to rely on another legal basis of processing. In the particular Member State where the controller is located, there are national laws that permits the bank to gather information from the public tax authorities directly, where the data subject consents to this beforehand.

The bank therefore presents information about the processing on the online application platform in such a manner that makes it easy for data subjects to understand what processing is mandatory and what is optional. The processing options, by default, do not allow retrieval of data directly from other sources than the data subject herself, and the option for direct information retrieval is presented in a manner that does not deter the data subject from abstaining. Any consent given to collect data directly from other controllers is a temporary right of access to a specific set of information.

Any given consent is processed electronically in a documentable manner, and data subjects are presented with an easy way of controlling what they have consented to and to withdraw their consent.

The controller has assessed these DPbDD requirements beforehand and includes all of these criteria in their requirements specification for the tender to procure the platform. The controller is aware that if they do not include the DPbDD requirements in the tender, it may either be too late or a very costly process to implement data protection afterwards.

### 3.3 Fairness

69. Fairness is an overarching principle which requires that personal data should not be processed in a way that is unjustifiably detrimental, unlawfully discriminatory, unexpected or misleading to the data

---

<sup>31</sup> See Article 6(1)(b) GDPR.

subject. Measures and safeguards implementing the principle of fairness also support the rights and freedoms of data subjects, specifically the right to information (transparency), the right to intervene (access, erasure, data portability, rectify) and the right to limit the processing (right not to be subject to automated individual decision-making and non-discrimination of data subjects in such processes).

70. Key design and default fairness elements may include:

- ✓ Autonomy – Data subjects should be granted the highest degree of autonomy possible to determine the use made of their personal data, as well as over the scope and conditions of that use or processing.
- ✓ Interaction – Data subjects must be able to communicate and exercise their rights in respect of the personal data processed by the controller.
- ✓ Expectation – Processing should correspond with data subjects' reasonable expectations.
- ✓ Non-discrimination – The controller shall not unfairly discriminate against data subjects.
- ✓ Non-exploitation – The controller should not exploit the needs or vulnerabilities of data subjects.
- ✓ Consumer choice – The controller should not “lock in” their users in an unfair manner. Whenever a service processing personal data is proprietary, it may create a lock-in to the service, which may not be fair, if it impairs the data subjects' possibility to exercise their right of data portability in accordance with Article 20.
- ✓ Power balance – Power balance should be a key objective of the controller-data subject relationship. Power imbalances should be avoided. When this is not possible, they should be recognised and accounted for with suitable countermeasures.
- ✓ No risk transfer – Controllers should not transfer the risks of the enterprise to the data subjects.
- ✓ No deception – Data processing information and options should be provided in an objective and neutral way, avoiding any deceptive or manipulative language or design.
- ✓ Respect rights – The controller must respect the fundamental rights of data subjects and implement appropriate measures and safeguards and not impinge on those rights unless expressly justified by law.
- ✓ Ethical – The controller should see the processing's wider impact on individuals' rights and dignity.
- ✓ Truthful – The controller must make available information about how they process personal data, they should act as they declare they will and not mislead the data subjects.
- ✓ Human intervention – The controller must incorporate *qualified* human intervention that is capable of uncovering biases that machines may create in accordance with the right to not be subject to automated individual decision making in Article 22.<sup>32</sup>
- ✓ Fair algorithms – Regularly assess whether algorithms are functioning in line with the purposes and adjust the algorithms to mitigate uncovered biases and ensure fairness in the processing. Data subjects should be informed about the functioning of the processing of personal data based on algorithms that analyse or make predictions about them, such as work performance, economic situation, health, personal preferences, reliability or behaviour, location or movements.<sup>33</sup>

---

<sup>32</sup> See Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. [https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc\\_id=49826](https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826)

<sup>33</sup> See Recital 71 GDPR.

### Example 1

A controller operates a search engine that processes mostly user-generated personal data. The controller benefits from having large amounts of personal data and being able to use that personal data for targeted advertisements. The controller therefore wishes to influence data subjects to allow more extensive collection and use of their personal data. Consent is to be collected by presenting processing options to the data subject.

When implementing the fairness principle, taking into account the nature, scope, context and purpose of the processing, the controller realizes that they cannot present the options in a way that nudges the data subject in the direction of allowing the controller to collect more personal data than if the options were presented in an equal and neutral way. This means that they cannot present the processing options in such a manner that makes it difficult for data subjects to abstain from sharing their data, or make it difficult for the data subjects to adjust their privacy settings and limit the processing. These are examples of dark patterns, which are contrary to the spirit of Article 25. The default options for the processing should not be invasive, and the choice for further processing should be presented in a manner that does not pressure the data subject to give consent. Therefore, the controller presents the options to consent or abstain as two equally visible choices, accurately representing the ramifications of each choice to the data subject.

### Example 2

Another controller processes personal data for the provision of a streaming service where users may choose between a regular subscription of standard quality and a premium subscription with higher quality. As part of the premium subscription, subscribers get prioritized customer service.

With regard to the fairness principle, the prioritized customer service granted to premium subscribers cannot discriminate the regular subscribers' access to exercise their rights according to the GDPR Article 12. This means that although the premium subscribers get prioritized service, such prioritization cannot result in a lack of appropriate measures to respond to request from regular subscribers without undue delay and in any event within one month of receipt of the requests.

Prioritized customers may pay to get better service, but all data subjects shall have equal and indiscriminate access to enforce their rights and freedoms as required under Article 12.

## 3.4 Purpose Limitation<sup>34</sup>

71. The controller must collect data for specified, explicit, and legitimate purposes, and not further process the data in a manner that is incompatible with the purposes for which they were collected.<sup>35</sup> The design of the processing should therefore be shaped by what is necessary to achieve the purposes. If any

<sup>34</sup> The Article 29 Working Party provided guidance for the understanding of the principle of purpose limitation under Directive 95/46/EC. Although the Opinion is not adopted by the EDPB, it may still be relevant as the wording of the principle is the same under the GDPR. Article 29 Working Party. "Opinion 03/2013 on purpose limitation". WP 203, 2 April 2013. [ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203\\_en.pdf](http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf)

<sup>35</sup> Art. 5(1)(b) GDPR.

further processing is to take place, the controller must first make sure that this processing has purposes compatible with the original ones and design such processing accordingly. Whether a new purpose is compatible or not, shall be assessed according to the criteria in Article 6(4).

72. 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.
- ✓ 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.

Example

The controller processes personal data about its customers. The purpose of the processing is to fulfil a contract, i.e. to be able to deliver goods to the correct address and obtain payment. The personal data stored is the purchase history, name, address, e-mail address and telephone number.

The controller is considering buying a Customer Relationship Management (CRM) product that gathers all the customer data about sales, marketing and customer service in one place. The product gives the opportunity of storing all phone calls, activities, documents, emails and marketing campaigns to get a 360-degree view of the customer. Moreover, the CRM is capable of automatically analysing the customers' purchasing power by using public information. The purpose of the analysis is to better target advertising activities. Those activities do not form part of the original lawful purpose of the processing.

To be in line with the principle of purpose limitation, the controller requires the provider of the product to map the different processing activities that use personal data to the purposes relevant for the controller.

After receiving the results of the mapping, the controller assesses whether the new marketing purpose and the targeted advertisement purpose are compatible with the original purposes defined when the data was collected, and whether there is a sufficient legal basis for the respective processing. If the assessment does not return a positive answer, the controller shall not proceed to use the respective functionalities. Alternatively, the controller could choose to forego the assessment and simply not make use of the described functionalities of the product.

### 3.5 Data Minimisation

73. Only personal data that is adequate, relevant and limited to what is **necessary** for the purpose shall be processed.<sup>36</sup> As a result, the controller has to predetermine which features and parameters of processing systems and their supporting functions are permissible. Data minimisation substantiates and operationalises the principle of necessity. In the further processing, the controller should periodically consider whether processed personal data is still adequate, relevant and necessary, or if the data shall be deleted or anonymized.
74. Controllers should first of all determine whether they even need to process personal data for their relevant purposes. The controller should verify whether the relevant purposes can be achieved by processing less personal data, or having less detailed or aggregated personal data or without having to process personal data at all<sup>37</sup>. Such verification should take place before any processing takes place, but could also be carried out at any point during the processing lifecycle. This is also consistent with Article 11.
75. Minimising can also refer to the degree of identification. If the purpose of the processing does not require the final set of data to refer to an identified or identifiable individual (such as in statistics), but the initial processing does (e.g. before data aggregation), then the controller shall delete or anonymize personal data as soon as identification is no longer needed. Or, if continued identification is needed for other processing activities, personal data should be pseudonymized to mitigate risks for the data subjects' rights.
76. Key design and default data minimisation elements may include:
  - ✓ Data avoidance – Avoid processing personal data altogether when this is possible for the relevant purpose.
  - ✓ Limitation – Limit the amount of personal data collected to what is necessary for the purpose
  - ✓ Access limitation – Shape the data processing in a way that a minimal number of people need access to personal data to perform their duties, and limit access accordingly.
  - ✓ Relevance – Personal data should be relevant to the processing in question, and the controller should be able to demonstrate this relevance.
  - ✓ Necessity – Each personal data category shall be necessary for the specified purposes and should only be processed if it is not possible to fulfil the purpose by other means.
  - ✓ Aggregation – Use aggregated data when possible.
  - ✓ Pseudonymization – Pseudonymize personal data as soon as it is no longer necessary to have directly identifiable personal data, and store identification keys separately.
  - ✓ Anonymization and deletion – Where personal data is not, or no longer necessary for the purpose, personal data shall be anonymized or deleted.
  - ✓ Data flow – The data flow should be made efficient enough to not create more copies than necessary.
  - ✓ “State of the art” – The controller should apply up to date and appropriate technologies for data avoidance and minimisation.

---

<sup>36</sup> Art. 5(1)(c) GDPR.

<sup>37</sup> Recital 39 GDPR so states: "...Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means."

### Example 1

A bookshop wants to add to their revenue by selling their books online. The bookshop owner wants to set up a standardised form for the ordering process. To ensure customers fill out all the wanted information the bookshop owner makes all of the fields in the form mandatory (if you don't fill out all the fields the customer can't place the order). The webshop owner initially uses a standard contact form, which asks information including the customer's date of birth, phone number and home address. However, not all the fields in the form are necessary for the purpose of buying and delivering the books. In this particular case, if the data subject pays for the product up front, the data subject's date of birth and phone number are not necessary for the purchase of the product. This means that these cannot be required fields in the web form to order the product, unless the controller can clearly demonstrate that it is otherwise necessary, and why the fields are necessary. Moreover, there are situations where an address will not be necessary. For example, when ordering an eBook the customer can download the product directly to their device.

The webshop owner therefore decides to make two web forms: one for ordering books, with a field for the customer's address and one web form for ordering eBooks without a field for the customer's address.

### Example 2

A public transportation company wishes to gather statistical information based on travellers' routes. This is useful for the purposes of making proper choices on changes in public transport schedules and proper routings of the trains. The passengers have to pass their ticket through a reader every time they enter or exit a means of transport. Having carried out a risk assessment related to the rights and freedoms of passengers' regarding the collection of passengers' travel routes, the controller establishes that it is possible to identify the passengers in circumstances where they live or work in scarcely populated areas, based on single route identification thanks to the ticket identifier. Therefore, since it is not necessary for the purpose of optimizing the public transport schedules and routings of the trains, the controller does not store the ticket identifier. Once the trip is over, the controller only stores the individual travel routes so as to not be able to identify trips connected to a single ticket, but only retains information about separate travel routes.

In cases where there can still be a risk of identifying a person solely by their public transportation travel route the controller implements statistical measures to reduce the risk, such as cutting the beginning and the end of the route.

### Example 3

A courier aims at assessing the effectiveness of its deliveries in terms of delivery times, workload scheduling and fuel consumption. In order to reach this goal, the courier has to process a number of personal data relating to both employees (drivers) and customers (addresses, items to be delivered, etc.). This processing operation entails risks of both monitoring employees, which requires specific legal safeguards, and tracking customers' habits through the knowledge of the delivered items over time. These risks can be significantly reduced with appropriate pseudonymization of employees and customers. In particular if pseudonymization keys are frequently rotated and macro areas are considered instead of detailed addresses, an effective data minimisation is pursued, and the controller

can solely focus on the delivery process and on the purpose of resource optimization, without crossing the threshold of monitoring individuals' (customers' or employees') behaviours.

#### Example 4

A hospital is collecting data about its patients in a hospital information system (electronic health record). Hospital staff needs to access patient files to inform their decisions regarding care for and treatment of the patients, and for the documentation of all diagnostic, care and treatment actions taken. By default, access is granted to only those members of the medical staff who are assigned to the treatment of the respective patient in the speciality department she or he is assigned to. The group of people with access to a patient's file is enlarged if other departments or diagnostic units are involved in the treatment. After the patient is discharged, and billing is completed, access is reduced to a small group of employees per speciality department who answer requests for medical information or a consultation made or asked for by other medical service providers upon authorization by the respective patient.

### 3.6 Accuracy

77. Personal data shall be accurate and kept up to date, and every reasonable step shall be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.<sup>38</sup>
78. The requirements should be seen in relation to the risks and consequences of the concrete use of data. Inaccurate personal data could be a risk to the data subjects' rights and freedoms, for example when leading to a faulty diagnosis or wrongful treatment of a health protocol, or an incorrect image of a person can lead to decisions being made on the wrong basis either manually, using automated decision-making, or through artificial intelligence.
79. Key design and default accuracy elements may include:
  - ]) Data source – Sources of personal data should be reliable in terms of data accuracy.
  - ]) Degree of accuracy – Each personal data element should be as accurate as necessary for the specified purposes.
  - ]) Measurably accurate - Reduce the number of false positives/negatives, for example biases in automated decisions and artificial intelligence.
  - ]) Verification – Depending on the nature of the data, in relation to how often it may change, the controller should verify the correctness of personal data with the data subject before and at different stages of the processing (e.g. to age requirements).
  - ]) Erasure/rectification – The controller shall erase or rectify inaccurate data without delay. The controller shall in particular facilitate this where the data subjects are or were children and later want to remove such personal data.<sup>39</sup>
  - ]) Error propagation avoidance – Controllers should mitigate the effect of an accumulated error in the processing chain.

---

<sup>38</sup> Art. 5(1)(d) GDPR.

<sup>39</sup> Cf. Recital 65.

- \_) Access – Data subjects should be given information about and effective access to personal data in accordance with the GDPR articles 12 to 15 in order to control accuracy and rectify as needed.
- \_) Continued accuracy – Personal data should be accurate at all stages of the processing, tests of accuracy should be carried out at critical steps.
- \_) Up to date – Personal data shall be updated if necessary for the purpose.
- \_) Data design - Use of technological and organisational design features to decrease inaccuracy, for example present concise predetermined choices instead of free text fields.

#### Example 1

An insurance company wishes to use artificial intelligence (AI) to profile customers buying insurance as a basis for their decision making when calculating the insurance risk. When determining how their AI solutions should be developed, they are determining the means of processing and shall consider data protection by design when choosing an AI application from a vendor and when deciding on how to train the AI.

When determining how to train the AI, the controller should have accurate data to achieve precise results. Therefore, the controller should ensure that the data used to train the AI is accurate.

Granted that they have a valid legal basis to train the AI using personal data from a large subset of their existing customers, the controller chooses a pool of customers that is representative of the population to also avoid bias.

The customer data is then collected from the respective data handling system, including data on the type of insurance, for example health insurance, home insurance, travel insurance, etc. as well as data from public registries they have lawful access to. All data are pseudonymized prior to transfer to the system dedicated to the training of the AI model.

To ensure that the data used for AI training is as accurate as possible, the controller only collects data from data sources with correct and up-to date information.

The insurance company tests whether the AI is reliable and provides non-discriminatory results both during its development and finally before the product is released. When the AI is fully trained and operative, the insurance company uses the results to support the insurance risk assessments, yet without solely relying on the AI to decide whether to grant insurance, unless the decision is made in accordance with the exceptions in Article 22 (2) GDPR.

The insurance company will also regularly review the results from the AI, to maintain the reliability and when necessary adjust the algorithm.

#### Example 2

The controller is a health institution looking to find methods to ensure the integrity and accuracy of personal data in their client registers.

In situations where two persons arrive at the institution at the same time and receive the same treatment, there is a risk of mistaking them if the only parameter to distinguish them is by name. To ensure accuracy, the controller needs a unique identifier for each person, and therefore more information than just the name of the client.

The institution uses several systems containing personal information of clients, and needs to ensure that the information related to the client is correct, accurate and consistent in all the systems at any point in time. The institution has identified several risks that may arise if information is changed in one system but not in the others.

The controller decides to mitigate the risk by using a hashing technique that can be used to ensure integrity of data in the treatment journal. Immutable cryptographic time stamps are created for treatment journal records and the client associated with them so that any changes can be recognized, correlated and traced if required.

### 3.7 Storage limitation

80. The controller must ensure that personal data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.<sup>40</sup> It is vital that the controller knows exactly what personal data the company processes and why. The purpose of the processing shall be the main criterion to decide in how long personal data shall be stored.
81. Measures and safeguards that implement the principle of storage limitation shall complement the rights and freedoms of the data subjects, specifically, the right to erasure and the right to object.
82. Key design and default storage limitation elements may include:
  - ) Deletion and anonymization – The controller should have clear internal procedures and functionalities for deletion and/or anonymization.
  - ) Effectiveness of anonymization/deletion – The controller shall make sure that it is not possible to re-identify anonymized data or recover deleted data, and should test whether this is possible.
  - ) Automation – Deletion of certain personal data should be automated
  - ) Storage criteria – The controller shall determine what data and length of storage is necessary for the purpose.
  - ) Justification – The controller shall be able to justify why the period of storage is necessary for the purpose and the personal data in question, and be able to disclose the rationale behind, and legal grounds for the retention period.
  - ) Enforcement of retention policies – The controller should enforce internal retention policies and conduct tests of whether the organization practices its policies.
  - ) Backups/logs – Controllers shall determine what personal data and length of storage is necessary for back-ups and logs.
  - ) Data flow – Controllers should beware of the flow of personal data, and the storage of any copies thereof, and seek to limit their “temporary” storage.

#### Example

The controller collects personal data where the purpose of the processing is to administer a membership of the data subject. The personal data shall be deleted when the membership is terminated and there is no legal basis for further storage of the data.

<sup>40</sup> Art. 5(1)(c) GDPR.

The controller first draws up an internal procedure for data retention and deletion. According to this, employees shall manually delete personal data after the retention period ends. The employee follows the procedure to regularly delete and correct data from any devices, from backups, logs, e-mails and other relevant storage media.

To make deletion more effective, and less error-prone, the controller then implements an automatic system instead, in order to delete data automatically, reliably and more regularly. The system is configured to follow the given procedure for data deletion which then occurs at a predefined regular interval to remove personal data from all of the company's storage media. The controller reviews and tests the retention procedure regularly and ensures that it concurs with the up-to-date retention policy.

### 3.8 Integrity and confidentiality

83. The principle of integrity and confidentiality includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. The security of personal data requires appropriate measures designed to prevent and manage data breach incidents; to guarantee the proper execution of data processing tasks, and compliance with the other principles; and to facilitate the effective exercise of individuals' rights.
84. Recital 78 states that one of the DPbDD measures could consist of enabling the controller to "*create and improve security features*". Along with other DPbDD measures, Recital 78 suggests a responsibility on the controllers to continually assess whether it is using the appropriate means of processing at all times and to assess whether the chosen measures actually counter the existing vulnerabilities. Furthermore, controllers should conduct regular reviews of the information security measures that surround and protect personal data, and the procedure for handling data breaches.
85. Key design and default integrity and confidentiality elements may include:
  - J Information security management system (ISMS) – Have an operative means of managing policies and procedures for information security.
  - J Risk analysis – Assess the risks against the security of personal data by considering the impact on individuals' rights and counter identified risks. For use in risk assessment; develop and maintain a comprehensive, systematic and realistic "threat modelling" and an attack surface analysis of the designed software to reduce attack vectors and opportunities to exploit weak points and vulnerabilities.
  - J Security by design – Consider security requirements as early as possible in the system design and development and continuously integrate and perform relevant tests.
  - J Maintenance – Regular review and test software, hardware, systems and services, etc. to uncover vulnerabilities of the systems supporting the processing.
  - J Access control management – Only the authorized personnel who need to should have access to the personal data necessary for their processing tasks, and the controller should differentiate between access privileges of authorized personnel.
    - o Access limitation (agents) – Shape the data processing in a way that a minimal number of people need access to personal data to perform their duties, and limit access accordingly.
    - o Access limitation (content) – In the context of each processing operation, limit access to only those attributes per data set that are needed to perform that operation.

- Moreover, limit access to data pertaining to those data subjects who are in the remit of the respective employee.
- Access segregation – Shape the data processing in a way that no individual needs comprehensive access to all data collected about a data subject, much less all personal data of a particular category of data subjects.
- 〕 Secure transfers – Transfers shall be secured against unauthorized and accidental access and changes.
- 〕 Secure storage – Data storage shall be secure from unauthorized access and changes. There should be procedures to assess the risk of centralized or decentralized storage, and what categories of personal data this applies to. Some data may need additional security measures than others or isolation from others.
- 〕 Pseudonymization – Personal data and back-ups/logs should be pseudonymized as a security measure to minimise risks of potential data breaches, for example using hashing or encryption.
- 〕 Backups/logs – Keep back-ups and logs to the extent necessary for information security, use audit trails and event monitoring as a routine security control. These shall be protected from unauthorised and accidental access and change and reviewed regularly and incidents should be handled promptly.
- 〕 Disaster recovery/ business continuity – Address information system disaster recovery and business continuity requirements to restore the availability of personal data following up major incidents.
- 〕 Protection according to risk – All categories of personal data should be protected with measures adequate with respect to the risk of a security breach. Data presenting special risks should, when possible, be kept separated from the rest of the personal data.
- 〕 Security incident response management – Have in place routines, procedures and resources to detect, contain, handle, report and learn from data breaches.
- 〕 Incident management – Controller should have processes in place to handle breaches and incidents, in order to make the processing system more robust. This includes notification procedures, such as management of notification (to the supervisory authority) and information (to data subjects).

Example

A controller wants to extract large quantities of personal data from a medical database containing electronic (patient) health records to a dedicated database server in the company in order to process the extracted data for quality assurance purposes. The company has assessed the risk for routing the extracts to a server that is accessible to all of the company's employees as likely to be high for data subjects' rights and freedoms. Since there is only one department in the company who needs to process the patient data extracts, the controller decides to restrict access to the dedicated server to employees in that department. Moreover, to further reduce risk, the data will be pseudonymized before they are transferred.

To regulate access and mitigate possible damage from malware, the company decides to segregate the network, and establish access controls to the server. In addition, they put up security monitoring and an intrusion detection and prevention system and isolates it from routine use. An automated auditing system is put in place to monitor access and changes. Reporting and automated alerts are generated from this when certain events related to usage are configured. The controller will ensure that users only have access on a need to know basis and with the appropriate access level. Inappropriate use can be quickly and easily detected.

Some of the extracts have to be compared with new extracts, and therefore are required to be stored for three months. The controller decides to put them into separate databases on the same server, and use both transparent and column-level encryption to store them. Keys for column data decryption are stored in dedicated security modules that can only be used by authorized personnel, but not extracted.

Handling upcoming incidents makes the system more robust, and reliable. The data controller understands that preventative and effective measures and safeguards should be built into all personal data processing it undertakes now and in the future, and that doing so may help prevent future such data breach incidents.

The controller establishes these security measures both to ensure accuracy, integrity and confidentiality, but also to prevent malware spread by cyber-attacks and to make the solution robust. Having robust security measures contributes to build trust with the data subjects.

### 3.9 Accountability<sup>41</sup>

86. The principle of accountability states that the controller shall be responsible for, and be able to demonstrate compliance with all of the abovementioned principles.
87. The controller needs to be able to demonstrate compliance with the principles. In doing so, the controller may demonstrate the effects of the measures taken to protect the data subjects' rights, and why the measures are considered to be appropriate and effective. For example, demonstrating why a measure is appropriate to ensure the principle of storage limitation in an effective manner.
88. To be able to process personal data responsibly, the controller should have both the knowledge of and the ability to implement data protection. This entails that the controller should understand their data protection obligations of the GDPR and be able to comply with these obligations.

## 4 ARTICLE 25(3) CERTIFICATION

89. According to Article 25(3), certification pursuant to Article 42 may be used as an element to demonstrate compliance with DPbDD. Conversely, documents demonstrating compliance with DPbDD may also be useful in a certification process. This means that where a processing operation by a controller or a processor has been certified as per Article 42, supervisory authorities shall take this into account in their assessment of compliance with the GDPR, specifically with regards to DPbDD.
90. When a processing operation by a controller or processor is certified according to Article 42, the elements that contribute to demonstrating compliance with Article 25(1) and (2) are the design processes, i.e. the process of determining the means of processing, the governance and the technical and organizational measures to implement the data protection principles. The data protection certification criteria are determined by the certification bodies or certification scheme owners and then approved by the competent supervisory authority or by the EDPB. For further information about certification mechanisms, we refer the reader to the EDPB Guideline on Certification<sup>42</sup> and other relevant guidance, as published on the EDPB website.

---

<sup>41</sup> See Recital 74, where controllers are required to demonstrate the effectiveness of their measures.

<sup>42</sup> EDPB. "Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation". Version 3.0, 4 June 2019.

[edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_guidelines\\_201801\\_v3.0\\_certificationcriteria\\_annex2\\_en.pdf](http://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf)

91. Even where a processing operation is awarded a certification in accordance with Article 42, the controller still has the responsibility to continuously monitor and improve compliance with the DPbDD-criteria of Article 25.

## 5 ENFORCEMENT OF ARTICLE 25 AND CONSEQUENCES

92. Supervisory authorities may assess compliance with Article 25 according to the procedures listed in Article 58. The corrective powers are specified in Article 58(2) and include the issuance of warnings, reprimands, orders to comply with data subjects' rights, limitations on or ban of processing, administrative fines, etc.
93. DPbDD is further a factor in determining the level of monetary sanctions for breaches of the GDPR, see Article 83(4).<sup>43</sup> <sup>44</sup>

## 6 RECOMMENDATIONS

94. Although not directly addressed in Article 25, processors and producers are also recognized as key enablers for DPbDD, they should be aware that controllers are required to only process personal data with systems and technologies that have built-in data protection.
95. When processing on behalf of controllers, or providing solutions to controllers, processors and producers should use their expertise to build trust and guide their customers, including SMEs, in designing /procuring solutions that embed data protection into the processing. This means in turn that the design of products and services should facilitate controllers' needs.
96. It should be kept in mind when implementing Article 25 that the main design objective is the *effective implementation* of the principles and *protection* of the rights of data subjects into the appropriate measures of the processing. In order to facilitate and enhance the adoption of DPbDD, we make the following recommendations to controllers as well as producers and processors:
- ]) Controllers should think of data protection from the *initial stages* of planning a processing operation, even before the time of determination of the means of processing.
  - ]) Where the controller has a Data Protection Officer (DPO), the EDPB encourages the active involvement of the DPO to integrate DPbDD in the procurement and development procedures, as well as in the whole processing life-cycle.
  - ]) A processing operation may be *certified*. The ability to get a processing operation certified provides an added value to a controller when choosing between different processing software, hardware, services and/or systems from producers or processors. Therefore, producers should strive to demonstrate DPbDD in the life-cycle of their development of a processing solution. A certification seal may also guide data subjects in their choice between different goods and services. Having the ability to get a processing certified can serve as a competitive advantage for producers, processors and controllers, and even enhances data subjects' trust in the

---

<sup>43</sup> Article 83(2)(d) GDPR stipulates that in determining the imposition of fines for breach of the GDPR "due regard" shall be taken of "the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32".

<sup>44</sup> More information on fines can be found in Article 29 Working Party. "Guidelines on application and setting of administrative fines for the purposes of the Regulation 2016/679". WP 253, 3 October 2017.  
[ec.europa.eu/newsroom/just/document.cfm?doc\\_id=47889](http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889) - endorsed by the EDPB.

processing of their personal data. If no certification is offered, controllers should seek to have other *guarantees* that producers or processors comply with the requirements of DPbDD.

- ) Controllers, processors and producers, should consider their obligations to provide children under 18 and other vulnerable groups with specific protection in complying with DPbDD.
- ) Producers and processors should seek to facilitate DPbDD implementation in order to support the controller's ability to comply with Article 25 obligations. Controllers, on the other hand, should not choose producers or processors who do not offer systems enabling or supporting the controller to comply with Article 25, because controllers will be held accountable for the lack of implementation thereof.
- ) Producers and processors should play an active role in ensuring that the criteria for the "state of the art" are met, and notify controllers of any changes to the "state of the art" that may affect the effectiveness of the measures they have in place. Controllers should include this requirement as a contractual clause to make sure they are kept up to date.
- ) The EDPB recommends controllers to require that producers and processors demonstrate how their hardware, software, services or systems enable the controller to comply with the requirements to accountability in accordance with DPbDD, for example by using key performance indicators to demonstrate the effectiveness of the measures and safeguards at implementing the principles and rights.
- ) The EDPB emphasizes the need for a harmonized approach to implement principles and rights in an effective manner and encourages associations or bodies preparing codes of conduct in accordance with Article 40 to also incorporate sector-specific guidance on DPbDD.
- ) Controllers should be fair to data subjects and transparent on how they assess and demonstrate effective DPbDD implementation, in the same manner as controllers demonstrate compliance with the GDPR under the principle of accountability.
- ) Privacy-enhancing technologies (PETs) that have reached the state-of-the-art maturity can be employed as a measure in accordance with the DPbDD requirements if appropriate in a risk based approach. PETs in themselves do not necessarily cover the obligations of Article 25. Controllers shall assess whether the measure is appropriate and effective in implementing the data protection principles and the rights of data subjects.
- ) Existing legacy systems are under the same DPbDD-obligations as new systems. If legacy systems do not already comply with DPbDD, and changes cannot be made to comply with the obligations, then the legacy system simply does not meet GDPR-obligations and cannot be used to process personal data.
- ) Article 25 does not lower the threshold of requirements for SMEs. The following points may facilitate SMEs' compliance with Article 25:
  - o Do early risk assessments
  - o Start with small processing – then scale its scope and sophistication later
  - o Look for producer and processor guarantees of DPbDD, such as certification and adherence to code of conducts
  - o Use partners with a good track record
  - o Talk with DPAs
  - o Read guidance from DPAs and the EDPB
  - o Adhere to codes of conduct where available
  - o Get professional help and advice

For the European Data Protection Board

The Chair

(Andrea Jelinek)

# Guidelines



## **Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR** **(part 1)**

**Version 2.0**

**Adopted on 7 July 2020**

## Version history

Version 2.0	7 July 2020	Adoption of the Guidelines after public consultation
Version 1.1	17 February 2020	Minor corrections
Version 1.0	2 December 2019	Adoption of the Guidelines for public consultation

## Table of contents

Introduction.....	4
1 The grounds of the Right to request delisting under GDPR .....	6
1.1 Ground 1: The Right to request delisting when the personal data are no longer necessary in relation to the search engine provider's processing (Article 17.1.a) .....	7
1.2 Ground 2: The Right to request delisting when the data subject withdraws consent where the legal basis for the processing is pursuant to Article 6.1.a or Article 9.2.a GDPR and where there is no other legal basis for the processing (Article 17.1.b) .....	7
1.3 Ground 3: The Right to request delisting when the data subject has exercised his or her Right to object to the processing of his or her personal data (Article 17.1.c) .....	8
1.4 Ground 4: The Right to request delisting when the personal data have been unlawfully processed (Article 17.1.d) .....	9
1.5 Ground 5: The Right to request delisting when the personal data have to be erased for compliance with a legal obligation (Article 17.1.e).....	10
1.6 Ground 6: The Right to request delisting when the personal data have been collected in relation to the offer of information society services (ISS) to a child (Article 17.1.f).....	10
2 The exceptions to the Right to request delisting under Article 17.3 .....	11
2.1 Processing is necessary for exercising the right of freedom of expression and information	11
2.2 Processing is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller .....	13
2.2.1 Legal obligation .....	13
2.2.2 Performance of a task carried out in public interest or in the exercise of official authority	14
2.3 Reasons of public interest in the area of public health.....	15
2.4 Archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89 (1) in so far as the Right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing.....	15
2.5 Establishment, exercise or defence of legal claims.....	16

# The European Data Protection Board

Having regard to Article 70 (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”),

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<sup>1</sup>,

Having regard to Article 12 and Article 22 of its Rules of Procedure,

## HAS ADOPTED THE FOLLOWING GUIDELINES

### INTRODUCTION

1. Following the Costeja judgment of the Court of Justice of the European Union (“CJEU”) of the 13th of May 2014<sup>2</sup>, a data subject may request the provider of an online search engine (“search engine provider”)<sup>3</sup>, to erase one or more links to web pages from the list of results displayed following a search made on the basis of his or her name.
2. According to Google’s Transparency Report<sup>4</sup>, the percentage of URLs that Google has not delisted has not increased over the past 5 years since that judgement. However, further to the CJEU judgement, data subjects seem to be more aware of their right to lodge a complaint for refusals of their delisting requests since Supervisory Authorities have observed an increase in the number of complaints regarding the refusal by search engine providers to delist links.
3. The European Data Protection Board (the “EDPB”), in accordance with its Action Plan, is developing guidelines in respect of Article 17 of the General Data Protection Regulation (“GDPR”). Until those guidelines are finalised, Supervisory Authorities must continue to handle and investigate, to the extent possible, complaints from data subjects and in a timely manner as possible.
4. Accordingly, this document aims to interpret the Right to be Forgotten in the search engines cases in light of the provisions of Article 17 GDPR (the “Right to request delisting”). Indeed, the Right to be Forgotten has been especially enacted under Article 17 GDPR to take into account the Right to request delisting established in the Costeja judgement.
5. Nonetheless, as under the Directive 95/46/EC of 24 October 1995 (the “Directive”) and as stated by the CJEU in its aforementioned Costeja judgement<sup>5</sup>, the Right to request delisting implies two rights

---

<sup>1</sup> References to “Member States” made throughout these guidelines should be understood as references to “EEA Member States”.

<sup>2</sup> CJEU, Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, judgment of 13 May 2014.

<sup>3</sup> including web archives such as archive.org

<sup>4</sup> <https://transparencyreport.google.com/eu-privacy/overview?hl=en>

<sup>5</sup> CJEU, Case C-131/12, judgment of 13 May 2014, paragraph 88: “Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, in order to comply with the rights laid down in those

(Right to Object and Right to Erasure GDPR). Indeed, the application of Article 21 is expressly foreseen as the third ground for the Right to erasure. As a result, both Article 17 and Article 21 GDPR can serve as a legal basis for delisting requests. The right to object and the right to obtain erasure were already granted under the Directive. Nonetheless, as it will be addressed, the wording of the GDPR requires an adjustment of the interpretation of these rights.

6. As a preliminary point, it should be noted that, while Article 17 GDPR is applicable to all data controllers, this paper focuses solely on processing by search engine providers and delisting requests submitted by data subjects.
7. There are some considerations when applying Article 17 GDPR in respect of a search engine provider's data processing. In this regard, it is necessary to state that the processing of personal data carried out in the context of the activity of the search engine provider must be distinguished from processing that is carried out by the publishers of the third-party websites such as media outlets that provide online newspaper content<sup>6</sup>.
8. If a data subject obtains the delisting of a particular content, this will result in the deletion of that specific content from the list of search results concerning the data subject when the search is, as a main rule, based on his or her name. This content will however still be available using other search criteria.
9. Delisting requests do not result in the personal data being completely erased. Indeed, the personal data will neither be erased from the source website nor from the index and cache of the search engine provider. For example, a data subject may seek the delisting of personal data from a search engine's index which have originated from a media outlet, such as a newspaper article. In this instance, the link to the personal data may be delisted from the search engine's index; however, the article in question will still remain within the control of the media outlet and may remain publicly available and accessible, even if no longer visible in search results based on queries that include in principle the data subject's name.
10. Nevertheless, search engine providers are not exempt in a general manner from the duty to fully erase. In some exceptional cases, they will need to carry out actual and full erasure in their indexes or caches. For example, in the event that search engine providers would stop respecting robots.txt requests implemented by the original publisher, they would actually have a duty to fully erase the URL to the content, as opposed to delist which is mainly based on data subject's name.
11. This paper is divided into two topics. The first topic concerns the grounds a data subject can rely on for a delisting request sent to a search engine provider pursuant to Article 17.1 GDPR. The second topic concerns the exceptions to the Right to request delisting according to Article 17.3 GDPR. This paper will be supplemented by an appendix dedicated to the assessment of criteria for handling complaints for refusals of delisting.

---

*provisions and in so far as the conditions laid down by those provisions are in fact satisfied, the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful".*

<sup>6</sup> CJEU, Case C 131/12, judgment of 13 May 2014; European Court of Human Rights (ECHR), "M.L. and W.W. vs Germany", 28 June 2018.

12. This paper does not address Article 17.2<sup>7</sup> GDPR. Indeed, this Article requires data controllers who have made the personal data public to inform controllers who have then reused those personal data through links, copies or replications. Such obligation of information does not apply to search engine providers when they find information containing personal data published or placed on the internet by third parties, index it automatically, store it temporarily and make it available to internet users according to a particular order of preference<sup>8</sup>. In addition, it does not require search engine providers, who have received a data subject's delisting request, to inform the third party which made public that information on the internet. Such obligation seeks to give greater responsibility to original controllers and try to prevent from multiplying data subjects' initiatives. In this regard, the statement by the Article 29 Working Party, saying that search engine providers "*should not as a general practice inform the webmasters of the pages affected by de-listing of the fact that some webpages cannot be accessed from the search engine in response to specific queries*" because "*such communication has no legal basis under EU data protection law*"<sup>9</sup> remains valid. It is also planned to have separate specific guidelines in respect of Article 17.2 GDPR.

## 1 THE GROUNDS OF THE RIGHT TO REQUEST DELISTING UNDER GDPR

13. The Right to request delisting as provided by Article 17 GDPR does not change the findings of the Costeja judgement, in which the CJEU held that a request for delisting was based on the Right to rectification/erasure and on the Right to object, pursuant to Article 12 and Article 14 of the Directive respectively.
14. Article 17.1 sets out a general principle to erase the data in the six following cases:
- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed (*Article 17.1.a*);
  - the data subject withdraws consent on which the processing is based (*Article 17.1.b*);
  - the data subject exercised his or her Right to object to processing of his or her personal data pursuant to Article 21.1 and 21.2 GDPR;
  - the personal data have been unlawfully processed (*Article 17.1.d*);
  - the erasure is compliant with a legal obligation (*Article 17.1.e*);
  - the personal data have been collected in relation to the offer of information society services to a minor (*Article 17.1.f* which refers to Article 8.1).
15. While all the grounds of Article 17 are theoretically applicable when it comes to delisting, in practice, some will be rarely or never used, such as in case of withdrawal of consent (see ground 2 below).
16. A data subject could however make a delisting request to a search engine provider based on more than one ground. For example, a data subject could request delisting because he or she considers it no

---

<sup>7</sup> Regulation 2016/679 (GDPR), Article 17.2: "*Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those data.*"

<sup>8</sup> See CJEU, Case C-136/17, GC and Others v CNIL, judgment of 24 September 2019, paragraph 35 and Case C-131/12, judgment of 13 May 2014, paragraph 41.

<sup>9</sup> Article 29 Data Protection Working Party, "Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12, WP 225, 26 November 2014, p. 23.

longer necessary that his or her personal data are processed by the search engine (Article 17.1.a) and also exercise his or her Right to object to the processing pursuant to Article 21.1 GDPR (Article 17.1.c).

17. In order for Supervisory Authorities to assess complaints regarding a search engine provider who has refused to erase a particular search result pursuant to Article 17 GDPR, Supervisory Authorities should establish whether the content to which an URL is referring to should be delisted or not. They should thus, in their analysis of the substance of the complaint, take into account the nature of the content made available by the publishers of the third-party websites.

#### **1.1 Ground 1: The Right to request delisting when the personal data are no longer necessary in relation to the search engine provider's processing (Article 17.1.a)**

18. According to Article 17.1.a GDPR, a data subject may request a search engine provider, following a search carried out as a general rule on the basis of his or her name, to delist content from its search results, where the data subject's personal data returned in those search results are no longer necessary in relation to the purposes of the processing by the search engine.
19. This provision enables a data subject to request the delisting of personal information concerning him or her that have been made accessible for longer than it is necessary for the search engine provider's processing. Yet, this processing is notably carried out for the purposes of making information more easily accessible for internet users. Within the context of the Right to request delisting, the balance between the protection of privacy and the interests of Internet users in accessing the information must be undertaken. In particular, it must be assessed whether or not, over the course of time, the personal data have become out-of-date or have not been updated.
20. For example, a data subject may exercise his or her Right to request delisting pursuant to Article 17.1.a when:
- information about him or her held by a company has been removed from the public register;
  - a link to a firm's website contains his or her contact details although he or she is no longer working in that firm;
  - information has to be published on the Internet for a number of years to meet a legal obligation and remained online longer than the time limit specified by the legislation.

21. As demonstrated by the examples, a data subject may notably request the delisting of a content where the personal information are obviously inaccurate due to the course of time, or outdated. Such an assessment will incidentally be dependent on the purposes of the original processing. Consequently, the original retention periods of personal data, when available, should also be considered by Supervisory Authorities when they conduct their analysis of delisting requests pursuant to Article 17.1.a GDPR.

#### **1.2 Ground 2: The Right to request delisting when the data subject withdraws consent where the legal basis for the processing is pursuant to Article 6.1.a or Article 9.2.a GDPR and where there is no other legal basis for the processing (Article 17.1.b)**

22. According to Article 17.1.b GDPR, a data subject may obtain the erasure of personal data concerning him or her where he or she withdraws consent for the processing.
23. In case of delisting, it would mean that the search engine provider would have utilised the consent of the data subject as lawful basis for its processing. Article 17.1 GDPR indeed raises the question of the

lawful basis for processing relied upon by a search engine provider for the purpose of returning search engine results including personal data.

24. For that reason, it appears unlikely that a delisting request would be submitted by a data subject on the basis that he or she wishes to withdraw consent because the controller to whom the data subject gave his or her consent is the web publisher, not the search engine operator that indexes the data. This interpretation has been endorsed by the CJEU in its judgement C-136-17 of 24 September 2019 (the “**Google 2 judgment**”).<sup>10</sup> The Court indicates that “*(...) the consent must be ‘specific’ and must therefore relate specifically to the processing carried out in connection with the activity of the search engine (...). In practice, it is scarcely conceivable (...) that the operator of a search engine will seek the express consent of data subjects before processing personal data concerning them for the purposes of his referencing activity. In any event, (...) the mere fact that a person makes a request for de-referencing means, in principle, at least at the time of making the request, that he or she no longer consents to the processing carried out by the operator of the search engine.*”
25. Nonetheless, in the event where a data subject would have withdrawn his or her consent for the use of his or her data on a particular web page, the original publisher of that web page should inform search engine providers who have indexed that data pursuant to Article 17.2 GDPR. The data subject would thus still be entitled to obtain the delisting of personal data concerning him or her but according to Article 17.1.c in such case.

### [1.3 Ground 3: The Right to request delisting when the data subject has exercised his or her Right to object to the processing of his or her personal data \(Article 17.1.c\)](#)

26. Pursuant to Article 17.1.c GDPR, a data subject can obtain from the search engine provider the erasure of personal data concerning him or her where he or she objects to the processing according to Article 21.1 GDPR and where there are no overriding legitimate grounds for the processing by the data controller.
27. The Right to object affords stronger safeguards to data subjects since it does not restrict the grounds according to which data subjects may request delisting as under Article 17.1 GDPR.
28. The Right to object to the processing was provided for by Article 14 of the Directive<sup>11</sup> and constituted a ground to request the delisting since the Costeja judgement. However, the differences in the wording of Article 21 GDPR and Article 14 of the Directive suggest that there may also be differences in their application.
29. Under the Directive, the data subject had to base his or her request “*on compelling legitimate grounds relating to his [or her] particular situation*”. In respect of the GDPR, a data subject can object to a processing “*on grounds relating to his or her particular situation*”. He or she thus no longer has to demonstrate “*compelling legitimate grounds*”.
30. The GDPR therefore changes the burden of proof, providing a presumption in favour of the data subject by obliging on the contrary the controller to demonstrate “*compelling legitimate grounds for the processing*” (Article 21.1). As a result, when a search engine provider receives a request to delist based on the data subject’s particular situation, it must now erase the personal data, pursuant to Article

---

<sup>10</sup> CJEU, Case C-136/17, Commission nationale de l’informatique et des libertés (CNIL) v. Google LLC, judgment of 24 September 2019.

<sup>11</sup> Directive 95/46/CE, Article 14: “*Member States shall grant the data subject the right: (a) at least in the cases referred to in Article 7(e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data*”

17.1.c GDPR, unless it can demonstrate “*overriding legitimate grounds*” for the listing of the specific search result, which read in conjunction with Article 21.1 are “*compelling legitimate grounds (...) which override the interests, rights and freedoms of the data subject*”. The search engine provider can establish any “*overriding legitimate grounds*”, including any exemption provided for under Article 17.3 GDPR. Nonetheless, if the search engine provider fails to demonstrate the existence of overriding legitimate grounds, the data subject is entitled to obtain the delisting pursuant to Article 17.1.c GDPR. As a matter of fact, delisting requests now imply to make the balance between the reasons related to the particular situation of the data subject and the compelling legitimate grounds of the search engine provider. The balance between the protection of privacy and the interests of Internet users in accessing to the information as ruled by the CJEU in the Costeja judgement can be relevant to conduct such assessment, as well as the balance operated by the European Court of Human Rights (ECHR) in press matters.

31. Therefore, the criteria of delisting developed by the Article 29 Working Party in guidelines on the implementation of the Court of Justice of the European Union judgment on “Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González” C-131/12 can still be used by search engine providers and Supervisory Authorities to assess a delisting request based on the Right to object (Article 17.1.c GDPR).
32. In this regard, the “*particular situation*” of the data subject will underlie the delisting request (for example, a search result creates detriment for a data subject when applying for jobs, or undermines his or her reputation in personal life) and will be taken into account when undertaking the balance between personal rights and right to information, in addition to the classic criteria for handling delisting requests, such as:
  - he or she does not play a role in public life;
  - the information at stake is not related to his or her professional life but affects his or her privacy;
  - the information constitutes hate speech, slander, libel or similar offences in the area of expression against him or her pursuant to a court order;
  - the data appears to be a verified fact but is factually inaccurate;
  - the data relates to a relatively minor criminal offence that happened a long time ago and causes prejudice to the data subject.
33. Nonetheless, these criteria won’t have to be examined in the absence of proof of compelling legitimate grounds to refuse the request.

#### [\*\*1.4 Ground 4: The Right to request delisting when the personal data have been unlawfully processed \(Article 17.1.d\)\*\*](#)

34. According to Article 17.1.d GDPR, a data subject may request the erasure of personal data concerning him or her in the instance where they have been unlawfully processed.
35. The notion of unlawful processing shall first be interpreted in view of Article 6 GDPR dedicated to lawfulness of processing. Other principles established under the GDPR (such as principles of Article 5 GDPR or of other provisions of Chapter II) may serve such interpretation.
36. This notion shall secondly be interpreted broadly, as the infringement of a legal provision other than the GDPR. Such interpretation must be conducted objectively by Supervisory Authorities, according to national laws or to a court decision. For instance, a delisting request shall be granted in the event where the listing of personal information has been expressly prohibited by a court order.

In cases where a search engine provider is not able to demonstrate a legal basis for its processing, a delisting request may fall under the scope of art 17.1.d GDPR, as the processing of personal data in such cases must be considered unlawful. Nonetheless, it must be reminded that in case of unlawfulness of the original processing, the data subject remains entitled to request delisting under Article 17.1.c GDPR.

### 1.5 Ground 5: The Right to request delisting when the personal data have to be erased for compliance with a legal obligation (Article 17.1.e)

37. According to Article 17.1.e GDPR, a data subject may request a search engine provider to delist one or more search results if the personal data need to be erased in compliance with a legal obligation in Union or Member State Law to which the search engine provider is subject.
38. Compliance with a legal obligation may result from an injunction, an express request by national or EU law for being under a “legal obligation to erase” or the mere breach by the search engine provider of the retention period. For illustrative purposes, the retention period of data is set by a text but would not be complied with (but this hypothesis mainly concerns public files). This case could maybe encompass the hypothesis of non-anonymized or identifying data available in open data.

### 1.6 Ground 6: The Right to request delisting when the personal data have been collected in relation to the offer of information society services (ISS) to a child (Article 17.1.f)

39. According to Article 17.1.f GDPR, a data subject may request a search engine provider to delist one or more results if personal data have been collected in relation to the offer of ISS to a child referred to in Article 8.1 GDPR.
40. The Article covers the direct provision of ISS and no other types of processing. The GDPR does not define ISS; rather, it refers to existing definitions in EU law<sup>12</sup>. There are some difficulties in interpretation as Recital 18 of Directive 2000/31/CE of the European Parliament and of the Council of June 8, 2000 provides a definition both broad and ambiguous of the notion of “*the direct provision of information society services*”. It mainly indicates that these services “*span a wide range of economic activities which take place on-line*”, but specifies that they are not restricted to “*services giving rise to on-line contracting but also, in so far as they represent an economic activity, extend to services which are not remunerated by those who receive them, such as those offering on-line information or commercial communications, or those providing tools allowing for search, access and retrieval of data*”, outlining the criteria of economic activity.
41. It stems from the above that search engine providers’ activities are likely to fall within the scope of direct provision of ISS. Nonetheless, search engine providers do not question whether the personal data they are indexing concern or not a child. Yet, in view of their specific responsibilities, and subject to the application of Article 17.3 GDPR, they would have to delist a content relating to a child pursuant to Article 17.1.c GDPR, acknowledging that being a child is a valid “ground relating to a particular situation” (Article 21 GDPR) and that “*children merit specific protection with regard to their personal data*” (Recital 38 GDPR). In such case, the context of the collection of personal data by the original

---

<sup>12</sup> Specifically, Article 1(1)(b) of Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification).

controller must be considered. In particular, the date of the beginning of the processing by the original website must be taken into account when a data subject requests the delisting of a content.

## 2 THE EXCEPTIONS TO THE RIGHT TO REQUEST DELISTING UNDER ARTICLE 17.3

42. Article 17.3 GDPR states that paragraphs 1 and 2 of Article 17 GDPR will not apply when processing is necessary:
- for exercising the right of freedom of expression and information (*Article 17.3.a*);
  - for compliance with a legal obligation that requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (*Article 17.3.b*);
  - for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9.2 as well as Article 9.3 (*Article 17.3.c*);
  - for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89 (1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing (*Article 17.3.d*); or
  - for the establishment, exercise or defense of legal claims (*Article 17.3.e*).
43. This part aims to demonstrate that most of the exceptions under Article 17.3 GDPR do not appear suitable in case of a delisting request. Such inadequacy pleads in favor of the application of Article 21 GDPR for delisting requests. In any event, it must be remembered that exceptions provided for under Article 17.3 GDPR can be invoked as compelling legitimate grounds pursuant to Article 17.1.c GDPR.

### 2.1 Processing is necessary for exercising the right of freedom of expression and information

44. This exemption to the application of Article 17.1 GDPR must be interpreted and applied in the context of the characteristics that define erasure. Article 17.1 GDPR is described as a clear and unconditional mandate addressed to controllers. If the conditions set forth in Article 17.1 GDPR are met, the controller shall "*have the obligation to delete personal data without undue delay*". Nonetheless, this is not an absolute right. The exemptions of Article 17.3 GDPR identify cases in which this obligation does not apply.
45. However, the balance between protecting the rights of interested parties and freedom of expression, including free access to information, is an intrinsic part of Article 17 GDPR.
46. The CJEU recognised in the Costeja judgement and repeated recently in the Google 2 judgment that the processing carried out by a search engine provider can significantly affect the fundamental rights to privacy and data protection law when the search is performed using the name of a data subject.
47. When weighing up the rights and freedoms of data subjects and the interests of Internet users in accessing the information through the search engine provider, the Court understood that "*Whilst it is true that the data subject's rights are protected by those articles also override, as a general rule, that interest of internet users, that balance may however depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the*

*public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life.”<sup>13</sup>*

48. The Court also considered that the rights of the data subjects will prevail, in general<sup>14</sup>, on the interest of Internet users in accessing information through the search engine provider. However, it identified several factors that may influence such determination. Among them include: the nature of the information or its sensitivity, and especially the interest of Internet users in accessing information, an interest that can vary depending on the role played by the interested party in public life.
49. The analysis of the delisting by the Court implies that, when assessing requests for delisting, the decision on the maintenance or blocking of the search results by a search engine provider necessarily has to consider what would be the impact of a delisting decision on the access to information by Internet users<sup>15</sup>. This impact does not necessarily entail the rejection of a delisting request. As confirmed by the Court, such interference with the fundamental rights of the data subject has to be justified by the preponderant interest of the general public in having access to the information in question.
50. The Court also distinguished between the legitimacy that a web publisher can have to disseminate information against the legitimacy of the search engine provider. The Court recognised that the activity of a web publisher can be undertaken exclusively for the purposes of journalism, in which case the web publisher would benefit from the exemptions that Member States could establish in these cases on the basis of Article 9 of the Directive (currently , Article 85.2 GDPR). In this regard, in the judgment “*M.L. and W.W. vs Germany*” of June 28th, 2018, the ECHR indicates that the balancing of the interests at issue may lead to different results depending on the request at stake (distinguishing (i) a request for erasure brought against the original publisher whose activity is at the heart of what freedom of expression aims to protect from (ii) a request brought against the search engine whose first interest is not to publish the original information on the data subject but notably to enable identifying any available information on this person and thus establishing his or her profile).
51. Those considerations should be assessed in respect of Article 17 GDPR complaints as in those decisions, the rights of the data subjects that have requested the delisting must be weighed with the interests of Internet users to access the information.
52. As explained by the CJEU in its Google 2 judgment, Article 17.3.a GDPR is “*an expression of the fact that the right to protection of personal data is not an absolute right but (...) must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality*”.<sup>16</sup> It “*expressly lays down the requirement to strike a balance between the fundamental rights to privacy and protection of personal data guaranteed by Articles 7 and 8 of the Charter, on the one hand, and the fundamental right of freedom of information guaranteed by Article 11 of the Charter, on the other.*”<sup>17</sup>
53. The Court concludes that “*where the operator of a search engine has received a request for de-referencing relating to a link to a web page on which personal data falling within the special categories (...), the operator must, on the basis of all the relevant factors of the particular case and taking into account the seriousness of the interference with the data subject’s fundamental rights to privacy and*

---

<sup>13</sup> CJEU, C-131/12, judgment of 13 May 2014, paragraph 81; CJEU, C-136/17, judgment of 24 September 2019, paragraph 66.

<sup>14</sup> CJEU, Case C-131/12, judgment of 13 May 2014, paragraph 99; CJEU, Case C-136/17, judgment of 24 September 2019, paragraph 53.

<sup>15</sup> CJEU, Case C-136/17, judgment of 24 September 2019, paragraph 56 et seq.

<sup>16</sup> CJEU, Case C-136/17, judgment of 24 September 2019, paragraph 57.

<sup>17</sup> CJEU, Case C-136/17, judgment of 24 September 2019, paragraph 59.

*protection of personal data laid down in Articles 7 and 8 of the Charter, ascertain, having regard to the reasons of substantial public interest (...), whether the inclusion of that link in the list of results displayed following a search on the basis of the data subject's name is strictly necessary for protecting the freedom of information of internet users potentially interested in accessing that web page by means of such a search, protected by Article 11 of the Charter.”<sup>18</sup>*

54. To conclude, depending on the circumstances of the case, search engine providers may refuse to delist a content in the event where they can demonstrate that its inclusion in the list of results is strictly necessary for protecting the freedom of information of internet users.

## 2.2 Processing is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

55. The content of this exemption makes it difficult to apply to the activity of search engine providers and it may have influence on the decisions of delisting certain results, as the processing of data by search engine providers is based, in principle, on the legitimate interest of the search engine provider.

### 2.2.1 Legal obligation

56. It is difficult to imagine the existence of legal provisions that oblige search engine providers to disseminate certain information. This is a consequence of the type of activity they develop. Search engine providers do not produce or present information.
57. Therefore, it seems unlikely that Member State law includes obligations for search engine providers to publish some type of information, instead of setting the obligation for that publication to be carried out in other web pages that will then be linked by search engine providers.
58. This assessment may also be extended to the possibility that Union or Member State law enables a public authority to take decisions that oblige search engine providers to publish information directly, and not through the URL links to the web page where that information is contained.
59. If there are cases in which the law of a Member State establishes the obligation for the search engine providers to publish decisions or documents containing personal information, or which authorises public authorities to demand such publication, the exemption contained in Article 17.3.b GDPR should be applied.
60. This application must take into account the terms in which it is established, that is, that the maintenance of the information in question is necessary to meet the legal obligation of publication. For example, that a legal obligation, or the decision of an authority legally entitled to adopt it, may include a time limit to the publication, or expressly stated purposes that may have been reached within a certain time period. In these cases, if the request for delisting occurs having exceeded these time limits, it should be considered that the exemption is no longer applicable.
61. On the contrary, it is frequent that Member State law provides for the publication on web pages of information containing personal data. That legal obligation to publish or maintain the published information cannot be considered as covered by the exemption contained in Article 17.3.b GDPR, since it is not directed to the search engine provider, but to the web publishers whose content is linked by

---

<sup>18</sup> CJEU, Case C-136/17, judgment of 24 September 2019, paragraph 69.

the search engine provider's index. Therefore, the search engine provider cannot invoke the existence of the obligation to reject a request for delisting.

62. However, the legal obligation of publication addressed to other web publishers should be taken into consideration when establishing the balance between the rights of data subjects and the interest of the Internet users in accessing the information. The fact that information must be published online by legal mandate, or following the decision of an authority legally entitled to adopt it, is indicative of an interest in the public being able to access that information.
63. That presumption of existence of a prevalent interest of the public does not operate in the same way in respect of the originating web pages compared to the results index of a search engine provider. Although the legal obligation to publish information on a certain web site may lead to the conclusion that this information should not be deleted from that web page, the decision regarding the results offered by the search engine provider when the name of a data subject is generally used as search term may be different.
64. The assessment of the request for delisting in these cases should not assume that the existence of the legal obligation of publication necessarily implies that, to the extent that this obligation is imposed on the original web publishers, it is not possible to accept the delisting by the search engine provider.
65. The decision should be taken, as is the general rule, by balancing the rights of the data subject and the interest of the Internet users to access this information through the search engine provider.

## 2.2.2 Performance of a task carried out in public interest or in the exercise of official authority

66. Search engine providers are not public authorities and therefore do not exercise public powers by themselves.
67. However, they could exercise those powers if they were attributed by the law of a Member State or of the Union. In the same way that they could carry out missions of public interest if their activity was considered necessary to satisfy that public interest in accordance with national legislation<sup>19</sup>.
68. Given the characteristics of search engine providers, it is unlikely that Member States will grant them public powers or consider that their activity or part of it is necessary for the achievement of a legally established public interest.
69. If, in spite of that, there is a case in which the law of the Member States grants search engines public powers or links their activity to the achievement of a public interest, they could avail of the exemption provided for in Article 17.3.b GDPR. The considerations previously made on the cases in which the law of a Member State had established a legal obligation to process information for search engine providers are also valid in this case.
70. To decide not to follow a delisting request for reasons related to this exemption, it is necessary to determine whether the maintenance of the information in the search engine results is necessary for the achievement of the public interest pursued or for the exercise of the powers of attorney.
71. On the other hand, the legal definition of powers or public interest would be carried out by a Member State, and if the search engine rejects a request for delisting on the basis of this exemption, it must

---

<sup>19</sup> GDPR, Article 6.3: "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 (...)"

also be understood that it does so because it considers that its activity is necessary to achieve public interests. The search engine provider should, in that event, provide reasons why it considers its activity to be carried out in the public interest. Without such an explanation, the denial to follow a data subject's delisting request does not have the possibility of relying on the exemption.

72. Consequently, it would also be the Supervisory Authority of the Member State whose law is applicable that will have to deal with a potential complaint pursuant to Article 55.2 GDPR.

### 2.3 Reasons of public interest in the area of public health

73. This exemption is a specific case based on the fact that processing is necessary for the performance of a public interest.
74. In this case, the public interest is limited to the area of public health, but, as with the public interest in any other area, the lawful basis for the processing must be established in Union law or Member State law.
75. From the point of view of the application of this exemption in the context of the activity of the search engine provider, the same conclusions as stated above can be reached. It does not seem likely that the law of a Member State or of the Union can establish a relationship between the activity of the search engine provider and the maintenance of information or of a category of information in the results of the search engine provider with the achievement of purposes of public interest in respect of public health.
76. This conclusion is more evident if one takes into account that the effect of delisting is only that some results are deleted from the results page that is obtained when mainly a name is entered as a search criterion. But the information is not deleted from the search engine providers' indexes and can be retrieved using other search terms.
77. It is, therefore, difficult to imagine that keeping those results visible when searches are mainly made on the basis of a data subject's name can be considered, in general, as something necessary for reasons of public interest in the area of public health.
78. The criteria on the applicability of national standards and the identification of the Supervisory Authority that must deal with possible claims in a case relating to Article 17 GDPR that was rejected using this exemption have been discussed above.

### 2.4 Archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89 (1) in so far as the Right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing

79. In this scenario, the search engine provider must be able to demonstrate that the delisting of a certain content on the results page is a serious obstacle or completely prevents the achievement of scientific or historical research purposes or statistical purposes.
80. It should be understood that these purposes must be objectively pursued by the search engine provider. The possibility that the suppression of results could significantly affect research purposes or statistical purposes pursued by users of the search engine provider's service is not relevant for the application of this exemption. Those purposes, if they exist, should be taken into consideration when establishing a balance between the rights of the data subject and the interests of the Internet users in accessing the information through the search engine provider.

81. It must also be noted that these purposes may be objectively pursued by the search engine provider, without a link between in principle the name of the data subject and the search results being necessary.

## [\*\*2.5 Establishment, exercise or defence of legal claims\*\*](#)

82. In principle, it is very unlikely that search engine providers can use this exemption to reject Article 17 GDPR delisting requests.
83. It must be further emphasised that a delisting request supposes the suppression of certain results from the search results page provided by the search engine provider when the name of a data subject is normally used as search criteria. The information remains accessible using other search terms.

# Guidelines



**Guidelines 01/2020 on processing personal data in the  
context of connected vehicles and mobility related  
applications**

**Version 2.0**

**Adopted on 9 March 2021**

## Version history

Version 2.0	9 March 2021	Adoption of the Guidelines after public consultation
Version 1.0	28 January 2020	Adoption of the Guidelines for public consultation

## Table of contents

1	INTRODUCTION .....	4
1.1	Related works.....	5
1.2	Applicable law .....	6
1.3	Scope .....	8
1.4	Definitions .....	11
1.5	Privacy and data protection risks .....	13
2	GENERAL RECOMMENDATIONS .....	15
2.1	Categories of data .....	15
2.2	Purposes.....	17
2.3	Relevance and data minimisation .....	17
2.4	Data protection by design and by default.....	18
2.5	Information.....	21
2.6	Rights of the data subject.....	23
2.7	Security.....	23
2.8	Transmitting personal data to third parties .....	24
2.9	Transfer of personal data outside the EU/EEA.....	25
2.10	Use of in-vehicle Wi-Fi technologies .....	26
3	CASE STUDIES .....	26
3.1	Provision of a service by a third party .....	26
3.2	eCall .....	30
3.3	Accidentology studies.....	33
3.4	Tackle auto theft .....	35

# The European Data Protection Board

Having regard to Article 70 (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”),

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<sup>1</sup>,

Having regard to Article 12 and Article 22 of its Rules of Procedure,

## HAS ADOPTED THE FOLLOWING GUIDELINES

### 1 INTRODUCTION

1. Symbol of the 20th century economy, the automobile is one of the mass consumer products that has impacted society as a whole. Commonly associated with the notion of freedom, cars are often considered as more than just a means of transportation. Indeed, they represent a private area in which people can enjoy a form of autonomy of decision, without encountering any external interferences. Today, as connected vehicles move into the mainstream, such a vision no longer corresponds to the reality. In-vehicle connectivity is rapidly expanding from luxury models and premium brands to high-volume midmarket models, and vehicles are becoming massive data hubs. Not only vehicles, but drivers and passengers are also becoming more and more connected. As a matter of fact, many models launched over the past few years on the market integrate sensors and connected on-board equipment, which may collect and record, among other things, the engine performance, the driving habits, the locations visited, and potentially even the driver’s eye movements, his or her pulse, or biometric data for the purpose of uniquely identifying a natural person.<sup>2</sup>
2. Such data processing is taking place in a complex ecosystem, which is not limited to the traditional players of the automotive industry, but is also shaped by the emergence of new players belonging to the digital economy. These new players may offer infotainment services such as online music, road condition and traffic information, or provide driving assistance systems and services, such as autopilot software, vehicle condition updates, usage-based insurance or dynamic mapping. Moreover, since vehicles are connected via electronic communication networks, road infrastructure managers and telecommunications operators involved in this process also play an important role with respect to the potential processing operations applied to the drivers’ and passengers’ personal data.
3. In addition, connected vehicles are generating increasing amounts of data, most of which can be considered personal data since they will relate to drivers or passengers. Even if the

---

<sup>1</sup> References to “Member States” made throughout this document should be understood as references to “EEA Member States”.

<sup>2</sup> Infographic “Data and the connected car” by the Future of Privacy Forum; [https://fpf.org/wp-content/uploads/2017/06/2017\\_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf](https://fpf.org/wp-content/uploads/2017/06/2017_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf)

data collected by a connected car are not directly linked to a name, but to technical aspects and features of the vehicle, it will concern the driver or the passengers of the car. As an illustration, data relating to the driving style or the distance covered, data relating to the wear and tear on vehicle parts, location data or data collected by cameras may concern driver behaviour as well as information about other people who could be inside or data subjects that pass by. Such technical data are produced by a natural person, and permit his/her direct or indirect identification, by the data controller or by another person. The vehicle can be considered as a terminal that can be used by different users. Therefore, as for a personal computer, this potential plurality of users does not affect the personal nature of the data.

4. In 2016, the Fédération Internationale de l'Automobile (FIA) ran a campaign across Europe called “My Car My Data” to get a sentiment on what Europeans think about connected cars.<sup>3</sup> While it showed the high interest of drivers for connectivity, it also highlighted the vigilance that must be exercised with regard to the use of the data produced by vehicles as well as the importance of complying with personal data protection legislation. Thus, the challenge is, for each stakeholder, to incorporate the “protection of personal data” dimension from the product design phase, and to ensure that car users enjoy transparency and control in relation to their data in accordance with recital 78 GDPR. Such an approach helps to strengthen user confidence, and thus the long-term development of those technologies.

## 1.1 Related works

5. Connected vehicles have become a substantial subject for regulators over the last decade, with a major increase in the last couple of years. Various works have thus been published at the national and international levels concerning the security and privacy of connected vehicles. Those regulations and initiatives aim at complementing the existing data protection and privacy frameworks with sector specific rules or providing guidance to professionals.

### 1.1.1 European-level and international initiatives

6. Since 31 March 2018, a 112-based eCall in-vehicle system is mandatory on all new types of M1 and N1 vehicles (passenger cars and light duty vehicles).<sup>4,5</sup> In 2006, the Article 29 Working Party had already adopted a working document on data protection and privacy implications in eCall initiative.<sup>6</sup> In addition, as previously discussed, the Article 29 Working Party also adopted an opinion in October 2017 regarding the processing of personal data in the context of Cooperative Intelligent Transport Systems (C-ITS).
7. In January 2017, the European Union Agency for Network and Information Security (ENISA) published a study focused on cyber security and resilience of smart cars listing the sensitive assets as well as the corresponding threats, risks, mitigation factors and possible security

---

<sup>3</sup> Campaign “My Car My Data”; <http://www.mycarmydata.eu/>.

<sup>4</sup> The interoperable EU-wide eCall; [https://ec.europa.eu/transport/themes/its/road/action\\_plan/ecall\\_en](https://ec.europa.eu/transport/themes/its/road/action_plan/ecall_en).

<sup>5</sup> Decision No 585/2014/EU of the European Parliament and of the Council of 15 May 2014 on the deployment of the interoperable EU-wide eCall service Text with EEA relevance; <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014D0585>.

<sup>6</sup> Working document on data protection and privacy implications in eCall initiative; [http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp125\\_en.pdf](http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp125_en.pdf).

measures to implement.<sup>7</sup> In September 2017, the International Conference of Data Protection and Privacy Commissioners (ICDPPC) adopted a resolution on connected vehicles.<sup>8</sup> Finally, in April 2018, the International Working Group on Data Protection in Telecommunications (IWGDPT), also adopted a working paper on connected vehicles.<sup>9</sup>

### 1.1.2 National initiatives of European Data Protection Board (EDPB) members

8. In January 2016, the Conference of the German Federal and State Data Protection Authorities and the German Association of the Automotive Industry (VDA) published a common declaration on the principles of data protection in connected and not-connected vehicles.<sup>10</sup> In August 2017, the UK Centre for Connected and Autonomous Vehicles (CCAV) released a guide stating principles of cyber security for connected and automated vehicles in order to raise awareness on the matter within the automotive sector.<sup>11</sup> In October 2017, the French data protection authority, the Commission Nationale de l'Informatique et des Libertés (CNIL), released a compliance package for connected cars in order to provide assistance to stakeholders on how to integrate data protection by design and by default, enabling data subjects to have effective control over their data.<sup>12</sup>

## 1.2 Applicable law

9. The relevant EU legal framework is the GDPR. It applies in any case where data processing in the context of connected vehicles involves processing personal data of individuals.
10. Additionally to the GDPR, directive 2002/58/EC as revised by 2009/136/EC (hereinafter – “ePrivacy directive”), **sets a specific standard for all actors that wish to store or access information stored in the terminal equipment of a subscriber or user in the European Economic Area (EEA).**
11. Indeed, if most of the ePrivacy directive provisions (art. 6, art. 9, etc.) only apply to providers of publicly available electronic communication services and providers of public communication networks, art. 5(3) ePrivacy directive is a general provision. It does not only apply to electronic communication services but also to every entity, private or public, that places on or reads information from a terminal equipment without regard to the nature of the data being stored or accessed.

---

<sup>7</sup> Cyber security and resilience of smart cars; <https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars>.

<sup>8</sup> Resolution on data protection in automated and connected vehicles;  
[https://edps.europa.eu/sites/edp/files/publication/resolution-on-data-protection-in-automated-and-connected-vehicles\\_en\\_1.pdf](https://edps.europa.eu/sites/edp/files/publication/resolution-on-data-protection-in-automated-and-connected-vehicles_en_1.pdf).

<sup>9</sup> Working paper on connected vehicles; <https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/working-paper/>.

<sup>10</sup> Data protection aspects of using connected and non-connected vehicles;  
[https://www.lda.bayern.de/media/dsk\\_joint\\_statement\\_vda.pdf](https://www.lda.bayern.de/media/dsk_joint_statement_vda.pdf).

<sup>11</sup> Principles of cyber security for connected and automated vehicles;  
<https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles>.

<sup>12</sup> Compliance package for a responsible use of data in connected cars; <https://www.cnil.fr/en/connected-vehicles-compliance-package-responsible-use-data>.

12. Regarding the notion of “*terminal equipment*”, the definition is given by directive 2008/63/CE<sup>13</sup>. Art. 1 (a) defines the terminal equipment as an “*equipment directly or indirectly connected to the interface of a public telecommunications network to send, process or receive information; in either case (direct or indirect), the connection may be made by wire, optical fibre or electromagnetically; a connection is indirect if equipment is placed between the terminal and the interface of the network; (b) satellite earth station equipment*”.
13. As a result, provided that the aforementioned criteria are met, the connected vehicle and device connected to it should be considered as a “*terminal equipment*” (just like a computer, a smartphone or a smart TV) and provisions of art. 5(3) ePrivacy directive apply where relevant.
14. As outlined by the EDPB in its opinion 5/2019 on the interplay between the ePrivacy directive and the GDPR,<sup>14</sup> art. 5(3) ePrivacy directive provides that, as a rule, and subject to the exceptions to that rule mentioned in paragraph 17 below, 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. To the extent that the information stored in the end-user’s device constitutes personal data, art. 5(3) ePrivacy directive shall take precedence over art. 6 GDPR with regards to the activity of storing or gaining access to this information.<sup>15</sup> Any processing operations of personal data following the aforementioned processing operations, including processing personal data obtained by accessing information in the terminal equipment, must have a legal basis under art. 6 GDPR in order to be lawful.<sup>16</sup>
15. Since the controller, when seeking consent for the storing or gaining of access to information pursuant to art. 5(3) ePrivacy directive, will have to inform the data subject about all the purposes of the processing – including any processing following the aforementioned operations (meaning the “*subsequent processing*”) – consent under art. 6 GDPR will generally be the most adequate legal basis to cover the processing of personal data following such operations (as far as the purpose of the following processing is comprehended by the data subject’s consent, see paragraphs 53-54 below). Hence, consent will likely constitute the legal basis both for the storing and gaining of access to information already stored and the subsequent processing of personal data<sup>17</sup>. Indeed, when assessing compliance with art. 6 GDPR, one should take into account that the processing as a whole involves specific activities for which the EU legislature has sought to provide additional protection.<sup>18</sup> Moreover, controllers must take into account the impact on data subjects’

---

<sup>13</sup> Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment (Codified version) (Text with EEA relevance); <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32008L0063>.

<sup>14</sup> European Data Protection Board, [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 (hereinafter - “Opinion 5/2019”), paragraph 40.

<sup>15</sup> Ibid, paragraph 40.

<sup>16</sup> Ibid, paragraph 41.

<sup>17</sup> Consent required by art. 5(3) of the “ePrivacy” directive and consent needed as a legal basis for the processing of data (art. 6 GDPR) for the same specific purpose can be collected at the same time (for example, by checking a box clearly indicating what the data subject is consenting to).

<sup>18</sup> Opinion 5/2019, paragraph 41.

rights when identifying the appropriate lawful basis in order to respect the principle of fairness.<sup>19</sup> The bottom line is that art. 6 GDPR cannot be relied upon by controllers in order to lower the additional protection provided by art. 5(3) ePrivacy directive.

16. The EDPB recalls that the notion of consent in the ePrivacy directive remains the notion of consent in the GDPR and must meet all the requirements of the consent as provided by art. 4(11) and 7 GDPR.
17. However, while consent is the principle, art. 5(3) ePrivacy directive allows the storing of information or the gaining of access to information that is already stored in the terminal equipment to be exempted from the requirement of informed consent, if it satisfies one of the following criteria:
  - ]) **Exemption 1:** for the sole purpose of carrying out the transmission of a communication over an electronic communications network;
  - ]) **Exemption 2:** when it is strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.
18. In such cases, the processing of personal data including personal data obtained by accessing information in the terminal equipment is based on one of the legal bases as provided by art. 6 GDPR. For example, consent is not needed when data processing is necessary to provide GPS navigation services requested by the data subject when such services can be qualified as information society services.

### 1.3 Scope

19. The EDPB would like to point out that these guidelines are intended to facilitate compliance of the processing of personal data carried out by a wide range of stakeholders working in this environment. However, they are not intended to cover all use cases possible in this context or to provide guidance for every possible specific situation.
20. The scope of this document focuses in particular on the personal data processing in relation to the non-professional use of connected vehicles by data subjects: e.g., drivers, passengers, vehicle owners, other road users, etc. More specifically, it deals with the personal data: (i) processed inside the vehicle, (ii) exchanged between the vehicle and personal devices connected to it (e.g., the user's smartphone) or (iii) collected locally in the vehicle and exported to external entities (e.g., vehicle manufacturers, infrastructure managers, insurance companies, car repairers) for further processing.
21. The connected vehicle definition has to be understood as a broad concept in this document. It can be defined as a vehicle equipped with many electronic control units (ECU) that are linked together via an in-vehicle network as well as connectivity facilities allowing it to share information with other devices both inside and outside the vehicle. As such, data can be exchanged between the vehicle and personal devices connected to it, for instance allowing the mirroring of mobile applications to the car's in-dash information and entertainment unit. Also, the development of standalone mobile applications, meaning independent of the vehicle (for example, relying on the sole use of the smart phone) to assist drivers is included

---

<sup>19</sup> European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 October 2019, paragraph 1.

in the scope of this document since they contribute to the vehicle's connectivity capacities even though they may not effectively rely on the transmission of data with the vehicle *per se*. Applications for connected vehicles are multiple and diverse and can include<sup>20</sup>:

22. *Mobility management*: functions that allow drivers to reach a destination quickly, and in a cost-efficient manner, by providing timely information about GPS navigation, potentially dangerous environmental conditions (e.g., icy roads), traffic congestion or road construction work, parking lot or garage assistance, optimised fuel consumption or road pricing.
23. *Vehicle management*: functions that are supposed to aid drivers in reducing operating costs and improving ease of use, such as notification of vehicle condition and service reminders, transfer of usage data (e.g., for vehicle repair services), customised “*Pay As/How You Drive*” insurances, remote operations (e.g., heating system) or profile configurations (e.g., seat position).
24. *Road safety*: functions that warn the driver of external hazards and internal responses, such as collision protection, hazard warnings, lane departure warnings, driver drowsiness detection, emergency call (eCall) or crash investigation “black-boxes” (event data recorder).
25. *Entertainment*: functions providing information to and involving the entertainment of the driver and passengers, such as smart phone interfaces (hands free phone calls, voice generated text messages), WLAN hot spots, music, video, Internet, social media, mobile office or “smart home” services.
26. *Driver assistance*: functions involving partially or fully automated driving, such as operational assistance or autopilot in heavy traffic, in parking, or on highways,
27. *Well-being*: functions monitoring the driver’s comfort, ability and fitness to drive such as fatigue detection or medical assistance.
28. Hence, vehicles can be natively connected or not and personal data can be collected through several means, including: (i) vehicle sensors, (ii) telematics boxes or (iii) mobile applications (e.g. accessed from a device belonging to a driver). In order to fall within the scope of this document, mobile applications need to be related to the environment of driving. For example, GPS navigation applications are in-scope. Applications whose functionalities only suggest places of interest (restaurants, historic monument, etc.) to drivers fall, however, outside the scope of these guidelines.
29. Much of the data that is generated by a connected vehicle relate to a natural person that is identified or identifiable and thus constitute personal data. For instance, data include directly identifiable data (e.g., the driver’s complete identity), as well as indirectly identifiable data such as the details of journeys made, the vehicle usage data (e.g., data relating to driving style or the distance covered), or the vehicle’s technical data (e.g., data relating to the wear and tear on vehicle parts), which, by cross-referencing with other files and especially the vehicle identification number (VIN), can be related to a natural person. Personal data in connected vehicles can also include metadata, such as vehicle maintenance status. In other words, any data that can be associated with a natural person therefore fall into the scope of this document.

---

<sup>20</sup> PwC Strategy 2014. “In the fast lane. The bright future of connected cars”: [https://www.strategyand.pwc.com/media/file/Strategyand\\_In-the-Fast-Lane.pdf](https://www.strategyand.pwc.com/media/file/Strategyand_In-the-Fast-Lane.pdf).

30. The connected vehicle ecosystem covers a wide spectrum of stakeholders. This ecosystem more precisely includes traditional actors of the automotive industry as well as emerging players from the digital industry. Hence, these guidelines are directed towards vehicle manufacturers, equipment manufacturers and automotive suppliers, car repairers, automobile dealerships, vehicle service providers, fleet managers, motor insurance companies, entertainment providers, telecommunication operators, road infrastructure managers and public authorities as well as data subjects. The EDPB underlines that the categories of data subjects will differ from one service to another (e.g., drivers, owners, passengers, etc.). This is a non-exhaustive list as the ecosystem entails a wide variety of services, including services for which a direct authentication or identification is needed and services for which this is not needed.
31. Some data processing performed by natural persons within the vehicle fall within "*the course of a purely personal or household activity*" and are consequently out of the scope of the GDPR<sup>21</sup>. In particular, this concerns the use of personal data within the vehicles by the sole data subjects who provided such data into the vehicle's dashboard. However, the EDPB recalls that according to its recital 18 the GDPR "*applies to controllers or processors which provide the means for processing personal data for such personal or household activities*".

### 1.3.1 Out of scope of this document

32. Employers providing company cars to members of their staff might want to monitor their employee's actions (e.g., in order to ensure the safety of the employee, goods or vehicles, to allocate resources, to track and bill a service or to check working time). Data processing carried out by employers in this context raises specific considerations to the employment context, which might be regulated by labour laws at the national level that cannot be detailed in these guidelines<sup>22</sup>.
33. While the data processing in the context of commercial vehicles used for professional purposes (such as public transport) and shared transport and MaaS solution may raise specific considerations which fall out of the scope of these general guidelines, many of the principles and recommendations set out here will also be applicable to those types of processing.
34. Connected vehicles being radio-enabled systems, they are subject to passive tracking such as Wi-Fi or Bluetooth tracking. In that sense they do not differ from other connected devices and fall in the scope of the ePrivacy directive which is currently being revised. This therefore excludes also large-scale tracking of Wi-Fi equipped vehicles<sup>23</sup> by a dense network of bystanders who use common smartphone location services. These routinely report all visible Wi-Fi networks to central servers. Since built-in Wi-Fi can be considered a secondary vehicle

---

<sup>21</sup> See GDPR, Article 2(2)(c).

<sup>22</sup> The Article 29 Working Party elaborated on this in its WP249 Opinion 2/2017 on data processing at work; [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=610169](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169).

<sup>23</sup> See for details: <https://www.datenschutzzentrum.de/artikel/1269-Location-Services-can-Systematically-Track-Vehicles-with-WiFi-Access-Points-at-Large-Scale.html>.

identifier<sup>24</sup>, this risks a systematic ongoing collection of complete vehicle movement profiles.

35. Vehicles are increasingly equipped with image recording devices (e.g., car parking camera systems or dashcams). Since this deals with the issue of filming public places, which requires an assessment of the relevant legislative framework which is specific to each Member State, this data processing is out of the scope of these guidelines.
36. The processing of data enabling Cooperative Intelligent Transport Systems (C-ITS) – as defined in the directive 2010/40/EU<sup>25</sup> has been dealt with in a specific opinion by the Article 29 Working Party<sup>26</sup>. While the definition of the C-ITS concept in the directive does not bear any technical specifications, the Article 29 Working Party focuses in its opinion on short-range communications, i.e. that do not involve the intervention of a network operator. More specifically, it provides analysis for specific use cases built for initial deployment and committed to assess at a later stage the new issues that will be undoubtedly raised when higher level of automation will be implemented. Since the data protection implications in the context of C-ITS are very specific (unprecedented amounts of location data, continuous broadcasting of personal data, exchange of data between vehicles and other road infrastructural facilities, etc.) and that it is still being discussed at the European level, the processing of personal data in that context is not covered by these guidelines.
37. Finally, this document does not aim to address all possible issues and questions raised by connected vehicles and can therefore not be considered as exhaustive.

#### 1.4 Definitions

38. The **processing** of personal data encompasses any operation that involves personal data 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, etc.<sup>27</sup>
39. The **data subject** is the natural person to whom the data covered by the processing relate. In the context of connected vehicles, it can, in particular, be the driver (main or occasional), the passenger, or the owner of the vehicle.<sup>28</sup>
40. The **data controller** is the person who determines the purposes and means of processing that take place in connected vehicles.<sup>29</sup> Data controllers can include service providers that process vehicle data to send the driver traffic-information, eco-driving messages or alerts

---

<sup>24</sup> Markus Ullmann, Tobias Franz, and Gerd Nolden, Vehicle Identification Based on Secondary Vehicle Identifier -- Analysis, and Measurements, in Proceedings, VEHICULAR 2017, The Sixth International Conference on Advances in Vehicular Systems, Technologies and Applications, Nice, France, July 23 to 27, 2017, p. 32-37.

<sup>25</sup> Directive 2010/40/EU of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport; <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010L0040>.

<sup>26</sup> Article 29 Working Party - Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS); [http://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=610171](http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610171).

<sup>27</sup> See GDPR, Article 4 (2).

<sup>28</sup> See GDPR, Article 4 (1).

<sup>29</sup> See GDPR, Article 4 (7) and the European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR (hereinafter - "Guidelines 07/2020").

regarding the functioning of the vehicle, insurance companies offering “*Pay As You Drive*” contracts, or vehicle manufacturers gathering data on the wear and tear affecting the vehicle’s parts to improve its quality. Pursuant to art. 26 GDPR, two or more controllers can jointly determine the purposes and means of the processing and thus be considered as joint controllers. In this case, they have to clearly define their respective obligations, especially as regards the exercising of the rights of data subjects and the provision of information as referred to in art. 13 and 14 GDPR.

41. The **data processor** is any person who processes personal data for and on behalf of the data controller.<sup>30</sup> The data processor collects and processes data on instruction from the data controller, without using those data for its own purposes. As an example, in a number of cases, equipment manufacturers and automotive suppliers may process data on behalf of vehicle manufacturers (which does not imply they cannot be a data controller for other purposes). In addition to requiring data processors to implement appropriate technical and organisational measures in order to guarantee a security level that is adapted to risk, art. 28 GDPR sets out data processors’ obligations.
42. The **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.<sup>31</sup> As an example, a commercial partner of the service provider that receives from the service provider personal data generated from the vehicle is a recipient of personal data. Whether they act as a new data controller or as a data processor, they shall comply with all the obligations imposed by the GDPR.
43. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients<sup>32</sup>; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing. As an example, law enforcement authorities are authorised third parties when they request personal data as part of an investigation in accordance with European Union or Member State law.

---

<sup>30</sup> See GDPR, Article 4 (8) and the Guidelines 07/2020.

<sup>31</sup> See GDPR, Article 4 (9) and the Guidelines 07/2020.

<sup>32</sup> GDPR, Article 4 (9) and Recital 31.

## 1.5 Privacy and data protection risks

44. Article 29 Working Party has already expressed several concerns about Internet of Things (IoT) systems that can also apply to connected vehicles.<sup>33</sup> The issues relating to data security and control already stressed regarding IoT are even more sensitive in the context of connected vehicles, since it entails road safety concerns – and can impact the physical integrity of the driver – in an environment traditionally perceived as isolated and protected from external interferences.
45. Also, connected vehicles raises significant data protection and privacy concerns regarding the processing of location data as its increasingly intrusive nature can put a strain on the current possibilities to remain anonymous. The EDPB wants to place particular emphasis and raise stakeholders' awareness to the fact that the use of location technologies requires the implementation of specific safeguards in order to prevent surveillance of individuals and misuse of the data.

### 1.5.1 Lack of control and information asymmetry

46. Vehicle drivers and passengers may not always be adequately informed about the processing of data taking place in or through a connected vehicle. The information may be given only to the vehicle owner, who may not be the driver, and may also not be provided in a timely fashion. Thus, there is a risk that there are insufficient functionalities or options offered to exercise the control necessary for affected individuals to avail themselves of their data protection and privacy rights. This point is of importance since, during their lifetime, vehicles may belong to more than one owner either because they are sold or because they are being leased rather than purchased.
47. Also, communication in the vehicle can be triggered automatically as well as by default, without the individual being aware of it. In the absence of the possibility to effectively control how the vehicle and its connected equipment interact, it is bound to become extraordinarily difficult for the user to control the flow of data. It will be even more difficult to control its subsequent use, and thereby prevent potential function creep.

### 1.5.2 Quality of the user's consent

48. The EDPB underlines that, when the data processing is based on consent, all elements of valid consent have to be met which means that consent shall be free, specific and informed and constitutes an unambiguous indication of the data subject's wishes as interpreted in EDPB guidelines on consent.<sup>34</sup> Data controllers need to pay careful attention to the modalities of obtaining valid consent from different participants, such as car owners or car users. Such consent must be provided separately, for specific purposes and may not be bundled with the contract to buy or lease a new car. Consent must be as easily withdrawn as it is given.
49. The same has to be applied when consent is required to comply with the ePrivacy directive, for example if there is a storing of information or the gaining of access to information already stored in the vehicle as required in certain cases by art. 5(3) of the ePrivacy directive. Indeed, as outlined above, consent in this context has to be interpreted in light of the GDPR.

---

<sup>33</sup> Article 29 Working Party – Opinion 8/2014 on the Recent Developments on the Internet of Things; [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf).

<sup>34</sup> European Data Protection Board, [Guidelines 05/2020 on consent under Regulation 2016/679](#), Version 1.1, 4 May 2020 (hereinafter - "Guidelines 05/2020").

50. In many cases, the user may not be aware of the data processing carried out in his/her vehicle. Such lack of information constitutes a significant barrier to demonstrating valid consent under the GDPR, as the consent must be informed. In such circumstances, consent cannot be relied upon as a legal basis for the corresponding data processing under the GDPR.
51. Classic mechanisms used to obtain individuals' consent may be difficult to apply in the context of connected vehicles, resulting in a "low-quality" consent based on a lack of information or in the factual impossibility to provide fine-tuned consent in line with the preferences expressed by individuals. In practice, consent might also be difficult to obtain for drivers and passengers who are not related to the vehicle's owner in the case of second-hand, leased, rented or borrowed vehicles.
52. When the ePrivacy directive does not require the data subject consent, the controller nonetheless has the responsibility of choosing the legal basis under art. 6 GDPR that is most appropriate to the case for the processing of personal data.

#### 1.5.3 Further processing of personal data

53. When data is collected on the basis of consent as required by art. 5(3) of the ePrivacy directive or on one of the exemptions of art. 5(3), and subsequently processed in accordance with art. 6 GDPR, it can only be further processed either if the controller seeks additional consent for this other purpose or if the data controller can demonstrate that it is based on a Union or Member State law to safeguard the objectives referred to in art. 23 (1) GDPR<sup>35</sup>. The EDPB considers that further processing on the basis of a compatibility test according to art. 6(4) GDPR is not possible in such cases, since it would undermine the data protection standard of the ePrivacy directive. Indeed, consent, where required under the ePrivacy directive, needs to be specific and informed, meaning that data subjects must be aware of each data processing purpose and entitled to refuse specific ones<sup>36</sup>. Considering that further processing on the basis of a compatibility test according to art. 6(4) of the GDPR is possible would circumvent the very principle of the consent requirements set forth by the current directive.
54. The EDPB recalls that the initial consent will never legitimise further processing as consent needs to be informed and specific to be valid.
55. For instance, telemetry data, which is collected during use of the vehicle for maintenance purposes may not be disclosed to motor insurance companies without the users consent for the purpose of creating driver profiles to offer driving behaviour-based insurance policies.
56. Furthermore, data collected by connected vehicles may be processed by law enforcement authorities to detect speeding or other infractions if and when the specific conditions in the law enforcement directive are fulfilled. In this case, such data will be considered as relating to criminal convictions and offences under the conditions laid down by art. 10 GDPR and any applicable national legislation. Manufacturers may provide the law enforcement authorities with such data if the specific conditions for such processing are fulfilled. The EDPB points out that processing of personal data for the sole purpose of fulfilling requests made by law enforcement authorities does not constitute a specified, explicit and legitimate purpose within the meaning of art. 5(1)(b) GDPR. When law enforcement authorities are authorized by law, they could be third parties within the meaning of art. 4(10) GDPR, in this case

---

<sup>35</sup> See also European Data Protection Board, Guidelines 10/2020 on restrictions under Article 23 GDPR.

<sup>36</sup> Guidelines 05/2020, sections 3.2 and 3.3.

manufacturers would be entitled to provide them with any data at their disposal subject to compliance with the relevant legal framework in each Member State.

#### 1.5.4 Excessive data collection

57. With the ever-increasing number of sensors being deployed in connected vehicles there is a very high risk of excessive data collection compared to what is necessary to achieve the purpose.
58. The development of new functionalities and more specifically those based on machine learning algorithms may require a large amount of data collected over a long period of time.

#### 1.5.5 Security of personal data

59. The plurality of functionalities, services and interfaces (e.g., web, USB, RFID, Wi-Fi) offered by connected vehicles increases the attack surface and thus the number of potential vulnerabilities through which personal data could be compromised. Unlike most IoT devices, connected vehicles are critical systems where a security breach may endanger the life of its users and people around. The importance of addressing the risk of hackers attempting to exploit connected vehicles' vulnerabilities is thus heightened.
60. In addition, personal data stored on vehicles and/or at external locations (e.g., in cloud computing infrastructures) must be adequately secured against unauthorized access. For instance, during maintenance, a vehicle has to be handed to a technician who will require access to some of the vehicle's technical data. While the technician needs to have access to the technical data, there is a possibility that the technician could attempt to access all the data stored in the vehicle.

## 2 GENERAL RECOMMENDATIONS

61. In order to mitigate the risks for data subjects identified above, the following general recommendations should be followed by vehicle and equipment manufacturers, service providers or any other stakeholder who may act as data controller or data processor in relation to connected vehicles.

### 2.1 Categories of data

62. As noted in the introduction, most data associated with connected vehicles will be considered personal data to the extent that it is possible to link it to one or more identifiable individuals. This includes technical data concerning the vehicle's movements (e.g., speed, distance travelled) as well concerning the vehicle's condition (e.g., engine coolant temperature, engine RPM, tyre pressure). Certain data generated by connected vehicles may also warrant special attention given their sensitivity and/or potential impact on the rights and interests of data subjects. At present, the EDPB has identified three categories of personal data warranting special attention, by vehicle and equipment manufacturers, service providers and other data controllers: location data, biometric data (and any special category of data as defined in art. 9 GDPR) and data that could reveal offences or traffic violations.

#### 2.1.1 Location data

63. When collecting personal data, vehicle and equipment manufacturers, service providers and other data controllers should keep in mind that location data are particularly revealing of the life habits of data subjects. The journeys carried out are very characteristic in that they

enable one to infer the place of work and of residence, as well as a driver's centres of interest (leisure), and may possibly reveal sensitive information such as religion through the place of worship, or sexual orientation through the places visited. Accordingly, the vehicle and equipment manufacturer, service provider and other data controller should be particularly vigilant not to collect location data except if doing so is absolutely necessary for the purpose of processing. As an example, when the processing consists in detecting the vehicle's movement, the gyroscope is sufficient to fulfil that function, without there being a need to collect location data.

64. In general, collecting location data is also subject to compliance with the following principles:

- ☐ adequate configuration of the frequency of access to, and of the level of detail of, location data collected relative to the purpose of processing. For example, a weather application should not be able to access the vehicle's location every second, even with the consent of the data subject;
- ☐ providing accurate information on the purpose of processing (e.g., is location history stored? If so, what is its purpose?);
- ☐ when the processing is based on consent, obtaining valid (free, specific and informed) consent that is distinct from the general conditions of sale or use, for example on the on-board computer;
- ☐ activating location only when the user launches a functionality that requires the vehicle's location to be known, and not by default and continuously when the car is started;
- ☐ informing the user that location has been activated, in particular by using icons (e.g., an arrow that moves across the screen);
- ☐ the option to deactivate location at any time;
- ☐ defining a limited storage period.

#### 2.1.2 Biometric data

65. In the context of connected vehicles, biometric data used for the purpose of uniquely identifying a natural person may be processed, within the remit of art. 9 GDPR and the national exceptions, among other things, to enable access to a vehicle, to authenticate the driver/owner, and/or to enable access to a driver's profile settings and preferences. When considering the use of biometric data, guaranteeing the data subject full control over his or her data involves, on the one hand, providing for the existence of a non-biometric alternative (e.g., using a physical key or a code) without additional constraint (that is, the use of biometrics should not be mandatory), and, on the other hand, storing and comparing the biometric template in encrypted form only on a local basis, with biometric data not being processed by an external reading/comparison terminal.

66. In the case of biometric data<sup>37</sup>, it is important to ensure that the biometric authentication solution is sufficiently reliable, in particular by complying with the following principles:

---

<sup>37</sup> The prohibition principle set out in article 9.1 GDPR only relates to "*biometric data for the purpose of uniquely identifying a natural person*".

- ☐ the adjustment of the biometric solution used (e.g., the rate of false positives and false negatives) is adapted to the security level of the required access control;
- ☐ the biometric solution used is based on a sensor that is resistant to attacks (such as the use of a flat-printed print for fingerprint recognition);
- ☐ the number of authentication attempts is limited;
- ☐ the biometric template/model is stored in the vehicle, in an encrypted form using a cryptographic algorithm and key management that comply with the state of the art;
- ☐ the raw data used to make up the biometric template and for user authentication are processed in real time without ever being stored, even locally.

### 2.1.3 Data revealing criminal offenses or other infractions

67. In order to process data that relate to potential criminal offences within the meaning of art. 10 GDPR, the EDPB recommends to resort to the local processing of the data where the data subject has full control over the processing in question (see discussion on local processing in section 2.4). Indeed – except for some exceptions (see the case study on accidentology studies presented below in section 3.3) – external processing of data revealing criminal offences or other infractions is forbidden. Thus, according to the sensitivity of the data, strong security measures such as those described in section 2.7 must be put in place in order to offer protection against the illegitimate access, modification and deletion of those data.
68. Indeed, some categories of personal data from connected vehicles could reveal that a criminal offence or other infraction has been or is being committed (“offence-related data”) and therefore be subject to special restrictions (e.g., data indicating that the vehicle crossed a white line, the instantaneous speed of a vehicle combined with precise location data). Notably, in the event that such data would be processed by the competent national authorities for the purposes of criminal investigation and prosecution of criminal offence, the safeguards provided for in art. 10 GDPR would apply.

## 2.2 Purposes

69. Personal data may be processed for a wide variety of purposes in relation to connected vehicles, including driver safety, insurance, efficient transportation, entertainment or information services. In accordance with the GDPR, data controllers must ensure that their purposes are “specified, explicit and legitimate”, not further processed in a way incompatible with those purposes and that there is a valid legal basis for the processing as required in art. 5 GDPR. Some concrete examples of purposes that may be pursued by data controllers operating in the context of connected vehicles are discussed in Part III of these guidelines, along with specific recommendations for each type of processing.

## 2.3 Relevance and data minimisation

70. To comply with the data minimization principle<sup>38</sup>, vehicle and equipment manufacturers, service providers and other data controllers should pay special attention to the categories of data they need from a connected vehicle, as they shall only collect personal data that are relevant and necessary for the processing. For instance, location data are particularly intrusive and can reveal many life habits of the data subjects. Accordingly, industry participants should be particularly vigilant not to collect location data except if doing so is

---

<sup>38</sup> GDPR, Article 5(1)(c).

absolutely necessary for the purpose of processing (see discussion on location data above, in section 2.1).

## 2.4 Data protection by design and by default

71. Taking into account the volume and diversity of personal data produced by connected vehicles, the EDPB notes that data controllers are required to ensure that technologies deployed in the context of connected vehicles are configured to respect the privacy of individuals by applying the obligations of data protection by design and by default as required by art. 25 GDPR. Technologies should be designed to minimize the collection of personal data, provide privacy-protective default settings and ensure that data subjects are well informed and have the option to easily modify configurations associated with their personal data. Specific guidance on how manufacturers and service providers can comply with data protection by design and by default could be beneficial for the industry and third party application providers.
72. Certain general practices, described below, can also help mitigate the risks to the rights and freedoms of natural persons associated with connected vehicles<sup>39</sup>.

### 2.4.1 Local processing of personal data

73. In general, vehicle and equipment manufacturers, service providers and other data controllers should, wherever possible, use processes that do not involve personal data or transferring personal data outside of the vehicle (i.e., the data is processed internally). The nature of connected vehicles however does present risks, such as the possibility of attacks on local processing by outside actors or local data being leaked by selling parts of the vehicle. Therefore, adequate attention and security measures should be taken into account to ensure that local processing shall remain local. This scenario offers the advantage of guaranteeing to the user the sole and full control of his/her personal data and, as such, it presents, “by design”, less privacy risks especially by prohibiting any data processing by stakeholders without the data subject knowledge. It also enables the processing of sensitive data such as biometric data or data relating to criminal offenses or other infractions, as well as detailed location data which otherwise would be subject to stricter rules (see below). In the same vein, it presents fewer cybersecurity risks and involves little latency, which makes it particularly suited to automated driving-assistance functions. Some examples of this type of solution could include:

- Z eco-driving applications that process data in the vehicle in order to display eco-driving advice in real time on the on-board screen;
- Z applications that involve a transfer of personal data to a device such as a smartphone under the user’s full control (via, for example, Bluetooth or Wi-Fi), and where the vehicle’s data are not transmitted to the application providers or the vehicle manufacturers; this would include, for instance, coupling of smartphones to use the car’s display, multimedia systems, microphone (or other sensors) for phone calls, etc., to the extent that the data collected remain under the control of the data subject and is exclusively used to provide the service he or she has requested;
- Z in-vehicle safety enhancing applications such as those that provide audible signals or vibrations of the steering wheel when a driver overtakes a car without indicating or straying over white

---

<sup>39</sup> See as well European Data Protection Board, [Guidelines 4/2019 on Article 25 Data Protection by Design and by Default](#), Version 2.0, adopted on 20 October 2020 (hereinafter - “Guidelines 4/2019”).

lines or which provides alerts as to the state of the vehicle (e.g., an alert on the wear and tear affecting brake pads);

- Z applications for unlocking, starting, and/or activating certain vehicle commands using the driver's biometric data that is stored within the vehicle (such as a face or voice models or fingerprint minutiae).

74. Applications such as the above involve processing carried out for the performance of purely personal activities by a natural person (i.e., without the transfer of personal data to a data controller or data processor). Therefore, in accordance with art. 2(2) GDPR, **these applications fall outside the scope of the GDPR.**

75. However, if the GDPR does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity, it does apply to controllers or processors, which provide the means for processing personal data for such personal or household activities (car manufacturers, service provider, etc.) in accordance with recital 18 GDPR. Hence, when they are acting as data controller or data processor, they must develop secure in-car application and with due respect to the principle of privacy by design and by default. In any case, according to recital 78 GDPR, "*When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations*".<sup>40</sup> One the one hand, it will enhance the development of user-centric services and, on the other hand, it will facilitate and secure any further uses in the future which could fall back within the scope of the GDPR. More specifically, the EDPB recommends developing a secure in-car application platform, physically divided from safety relevant car functions so that the access to car data does not depend on unnecessary external cloud capabilities.

76. Local data processing should be considered by car manufacturers and service providers, whenever possible, to mitigate the potential risks of cloud processing, as they are underlined in the opinion on Cloud Computing released by the Article 29 Working Party.<sup>41</sup>

77. In general users should be able to control how their data are collected and processed in the vehicle:

- Z information regarding the processing must be provided in the driver's language (manual, settings, etc.);
- Z the EDPB recommends that only data strictly necessary for the functioning of the vehicle are processed by default. Data subjects should have the possibility to activate or deactivate the data processing for each other purpose and controller/processor and have the possibility to delete the data concerned, taking into account the purpose and the legal basis of the data processing ;

---

<sup>40</sup> For more recommendations on privacy by design and privacy by default see also Guidelines 4/2019.

<sup>41</sup> Article 29 Working Party – Opinion 5/2012 on Cloud Computing; [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf).

- ☐ data should not be transmitted to any third parties (i.e., the user has sole access to the data);
- ☐ data should be retained only for as long as is necessary for the provision of the service or otherwise required by Union or Member State law;
- ☐ data subjects should be able to delete permanently any personal data before the vehicles are put up for sale;
- ☐ data subjects should, where feasible, have a direct access to the data generated by these applications.

78. Finally, while it may not always be possible to resort to local data processing for every use-case, “hybrid processing” can often be put in place. For instance, in the context of usage-based insurance, personal data regarding driving behaviour (such as the force exerted on the brake pedal, mileage driven, etc.) could either be processed inside the vehicle or by the telematics service provider on behalf of the insurance company (the data controller) to generate numerical scores that are transferred to the insurance company on a defined basis (e.g. on a monthly basis). In this way, the insurance company does not gain access to the raw behavioural data but only to the aggregate score that is the result of the processing. This ensures that principles of data minimization are satisfied by design. This also means that users must have the ability to exercise their right when data are stored by other parties: for example, a user should have the ability to delete data stored in the systems of a car maintenance shop or dealership under the conditions of art.17 GDPR.

#### 2.4.2 Anonymization and pseudonymisation

79. If the transmission of personal data outside the vehicle is envisaged, consideration should be given to anonymize them before being transmitted. When anonymising the controller should take into account all processing involved which could potentially lead to re-identification of data, such as the transmission of locally anonymised data. The EDPB recalls that the principles of data protection do not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable<sup>42</sup>. Once a dataset is truly anonymised and individuals are no longer identifiable, European data protection law no longer applies. As a consequence, anonymisation, where relevant, may be a good strategy to keep the benefits and to mitigate the risks in relation to connected vehicles.

80. As detailed in the opinion by the Article 29 Working Party on anonymization techniques, various methods can be used – sometimes in combination – in order to reach data anonymisation.<sup>43</sup>

81. Other techniques such as pseudonymisation<sup>44</sup> can help minimize the risks generated by the data processing, taking into account that in most cases, directly identifiable data are not necessary to achieve the purpose of the processing. Pseudonymisation, if reinforced by security safeguards, improves the protection of personal data by reducing the risks of

---

<sup>42</sup> See GDPR, Article 4 (1) and Recital 26.

<sup>43</sup> WP29 - Opinion 05/2014 on Anonymisation Techniques; [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf).

<sup>44</sup> GDPR, Article 4 (5). Enisa report on December 03, 2019:

<https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices>.

misuse. Pseudonymisation is reversible, unlike anonymisation, and pseudonymised data are considered as personal data subject to the GDPR.

#### 2.4.3 Data protection impact assessments

82. Given the scale and sensitivity of the personal data that can be generated *via* connected vehicles; it is likely that processing – particularly in situations where personal data are processed outside of the vehicle - will often result in a high risk to the rights and freedoms of individuals. Where this is the case, industry participants will be required to perform a data protection impact assessment (DPIA) to identify and mitigate the risks as detailed in art. 35 and 36 GDPR. Even in the cases where a DPIA is not required, it is a best practice to conduct one as early as possible in the design process. This will allow industry participants to factor the results of this analysis into their design choices prior to the roll-out of new technologies.

### 2.5 Information

83. Prior to the processing of personal data, the data subject shall be informed of the identity of the data controller (e.g., the vehicle and equipment manufacturer or service provider), the purpose of processing, the data recipients, the period for which data will be stored, and the data subject's rights under the GDPR<sup>45</sup>.

84. In addition, the vehicle and equipment manufacturer, service provider or other data controller should also provide the data subject with the following information, in clear, simple, and easily-accessible terms:

- ☐ the contact details of the data protection officer;
- ☐ the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- ☐ the explicit mention of the legitimate interests pursued by the data controller or by a third party, when such legitimate interests constitute the legal basis for processing;
- ☐ the recipients or categories of recipients of the personal data, if any;
- ☐ the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- ☐ the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- ☐ the existence of the right to withdraw consent at any time without affecting the lawfulness of processing based on consent before its withdrawal where the processing is based on consent;
- ☐ where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and safeguards used to transfer them;
- ☐ whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

---

<sup>45</sup> GDPR, Article 5 (1) (a) and 13. See also Article 29 Working Party, [Guidelines on Transparency under Regulation 2016/679](#) (wp260rev.01), endorsed by the EDPB.

- Z the existence of automated decision-making, including profiling that produces legal effects concerning the data subject or similarly significantly affects the data subject, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. This could particularly be the case in relation to the provision of usage-based insurance to individuals;
  - Z the right to lodge a complaint with a supervisory authority;
  - Z information about further processing;
  - Z In case of joint data controllership, clear and complete information about the responsibilities of each data controller.
85. In some cases, personal data is not collected directly from the individual concerned. For instance, a vehicle and equipment manufacturer may rely on a dealer to collect information about the owner of the vehicle in order to offer an emergency road side assistance service. When data have not been collected directly, the vehicle and equipment manufacturer, service provider or other data controller shall, in addition to the information mentioned above, also indicate the categories of personal data concerned, the source from which the personal data originate, and, if applicable, whether those data came from publicly accessible sources. That information must be provided by the controller within a reasonable period after obtaining the data, and **no later than the first of the following dates** in accordance with art. 14 (3) GDPR: (i) one month after the data are obtained, having regard to the specific circumstances in which the personal data are processed, (ii) upon first communication with the data subject, or (iii) if those data are transmitted to a third party, before the transmission of the data.
86. New information may also need to be provided to data subjects when they are taken care of by new data controller. A roadside assistance service that interacts with connected vehicles can be provided by different data controllers depending in which country or region the assistance is required. New data controllers should provide data subjects with the required information when data subjects cross borders and services that interact with connected vehicles are provided by new data controllers.
87. The information directed to the data subjects may be provided in layers<sup>46</sup>, i.e. by separating two levels of information: on the one hand, first-level information, which is the most important for the data subjects, and, on the other hand, information that presumably is of interest at a later stage. The essential first-level information includes, in addition to the identity of the data controller, the purpose of the processing and a description of the data subject's rights, as well as any additional information on the processing which has the most impact on the data subject and processing which could surprise them. The EDPB recommends that, in the context of connected vehicles, the data subject should be made aware of all the recipients in the first layer of information. As stated in the WP29 guidelines on transparency, controllers should provide information on the recipients that is most meaningful for data subjects. In practice, this will generally be the named recipients, so that data subjects know exactly who has their personal data. If controllers cannot provide the names of the recipients, the information should be as specific as possible by indicating the

---

<sup>46</sup> See Article 29 Working Party, [Guidelines on Transparency under Regulation 2016/679 \(wp260rev.01\)](#), endorsed by the EDPB.

type of recipient (i.e. by reference to the activities it carries out), the industry, sector and sub-sector, and the location of the recipients.

88. The data subjects may be informed by concise and easily understandable clauses in the contract of sale of the vehicle, in the contract for the provision of services, and/or in any written medium, by using distinct documents (e.g., the vehicle's maintenance record book or manual) or the on-board computer.
89. Standardised icons could be used in addition to the information necessary, as required under art. 13 and 14 GDPR, to enhance transparency by potentially reducing the need for vast amounts of written information to be presented to a data subject. It should be visible in vehicles in order to provide, in relation to the planned processing, a good overview that is understandable, and clearly legible. The EDPB emphasises the importance of standardising those icons, so that the user finds the same symbols regardless of the make or model of the vehicle. For example, when certain types of data are being collected, such as location, the vehicles could have a clear signal on-board (such as a light inside the vehicle) to inform passengers about data collection.

## 2.6 Rights of the data subject

90. Vehicle and equipment manufacturers, service providers and other data controllers should facilitate data subjects' control over their data during the entire processing period, through the implementation of specific tools providing an effective way to exercise their rights, in particular their right of access, rectification, erasure, their right to restrict the processing and, depending on the legal basis of the processing, their right to data portability and their right to object.
91. To facilitate settings modifications, a profile management system should be implemented in order to store the preferences of known drivers and help them to change easily their privacy settings anytime. The profile management system should centralize every data setting for each data processing, especially to facilitate the access, deletion, removal and portability of personal data from vehicle systems at the request of the data subject. Drivers should be enabled to stop the collection of certain types of data, temporarily or permanently, at any moment, unless there is a specific legal ground that the controller can rely on to continue the collection of specific data. In case of a contract that provides a personalized offer based on driving behaviour this may mean that the user as a result should be reverted to the standard conditions of that contract. These features should be implemented inside the vehicle, although it could also be provided to data subjects through additional means (e.g., dedicated application). Furthermore, in order to allow data subjects to quickly and easily remove personal data that can be stored on the car's dashboard (for example, GPS navigation history, web browsing, etc.), the EDPB recommends that manufacturers provide a simple functionality (such as a delete button).
92. The sale of a connected vehicle and the ensuing change of ownership should also trigger the deletion of any personal data, which is no longer needed for the previous specified purposes and the data subject should be able to exercise his or her right to portability.

## 2.7 Security

93. Vehicle and equipment manufacturers, service providers and other data controllers should put in place measures that guarantee the security and confidentiality of processed data and

take all useful precautions to prevent control being taken by an unauthorised person. In particular, industry participants should consider adopting the following measures:

- Z encrypting the communication channels by means of a state-of-the-art algorithm;
- Z putting in place an encryption-key management system that is unique to each vehicle, not to each model;
- Z when stored remotely, encrypting data by means of state-of-the-art algorithms;
- Z regularly renewing encryption keys;
- Z protecting encryption keys from any disclosure;
- Z authenticating data-receiving devices;
- Z ensuring data integrity (e.g., by hashing);
- Z make access to personal data subject to reliable user authentication techniques (password, electronic certificate, etc.);

94. Concerning more specifically vehicle manufacturers, the EDPB recommends the implementation of the following security measures:

- Z partitioning the vehicle's vital functions from those always relying on telecommunication capacities (e.g., "infotainment");
- Z implementing technical measures that enable vehicle manufacturers to rapidly patch security vulnerabilities during the entire lifespan of the vehicle;
- Z for the vehicle's vital functions, give priority as much as possible to using secure means of communications that are specifically dedicated to transportation;
- Z setting up an alarm system in case of attack on the vehicle's systems, with the possibility of operating in downgraded mode<sup>47</sup>;
- Z storing a log history of any access to the vehicle's information system, e.g. going back six months as a maximum period, in order to enable the origin of any potential attack to be understood and periodically carry out a review of the logged information to detect possible anomalies.

95. These general recommendations should be completed by specific requirements taking into account the characteristics and purpose of each data processing.

## 2.8 Transmitting personal data to third parties

96. In principle, only the data controller and the data subject have access to the data generated by a connected vehicle. However, the data controller may transmit personal data to a commercial partner (recipient), to the extent that such transmission lawfully relies on one of the legal bases stated in art. 6 GDPR.

---

<sup>47</sup> Downgraded mode is a vehicle operating mode ensuring that the functions essential for the safe operation of the vehicle (i.e., minimum safety requirements) would be guaranteed, even if other less important functionalities would be deactivated (e.g., the operation of the geo-guidance device can be considered as non-essential, as opposed to the braking system).

97. In view of the possible sensitivity of the vehicle-usage data (e.g., journeys made, driving style), the EDPB recommends that the data subject's consent be systematically obtained before their data are transmitted to a commercial partner acting as a data controller (e.g., by ticking a box that is not pre-ticked, or, where technically possible, by using a physical or logical device that the person can access from the vehicle). The commercial partner in turn becomes responsible for the data that it receives, and is subject to all the provisions of the GDPR.
98. The vehicle manufacturer, service provider or other data controller can transmit personal data to a data processor selected to play a part in providing the service to the data subject, provided the data processor shall not use those data for its own purpose. Data controllers and data processors shall draw up a contract or other legal document specifying the obligations of each party and setting out the provisions of art. 28 GDPR.

## 2.9 Transfer of personal data outside the EU/EEA

99. When personal data is transferred outside the European Economic Area, special safeguards are foreseen to ensure that the protection travels with the data.
100. As a consequence, the data controller may transfer personal data to a recipient only to the extent that such transfer is in accordance with the requirements laid down in Chapter V GDPR.

## 2.10 Use of in-vehicle Wi-Fi technologies

101. Advances in cellular technology have made it possible to easily use the Internet on the road. While it is possible to get Wi-Fi connectivity in a vehicle through a smartphone hotspot or a dedicated device (OBD-II dongle, wireless modem or router, etc.), most manufacturers offer nowadays models that include a built-in cellular data connection and are also capable of creating Wi-Fi networks. Depending on the case, various aspects must be considered:

ZThe Wi-Fi connectivity is offered as a service by a road professional, such as a taxi driver for its customers. In this case, the professional or his/her company might be considered as an internet service provider (ISP), hence be subject to specific obligations and restrictions regarding the processing of his / her clients' personal data.

ZThe Wi-Fi connectivity is put in place for the sole use of the driver (at the exclusion of the driver and his/her passengers). In this case, the processing of personal data is considered to be purely personal or household activity in accordance with art. 2(2)(c) and recital 18 GDPR.

102. In general, the proliferation of Internet connection interfaces via Wi-Fi poses greater risks to the privacy of individuals. Indeed, through their vehicles, users become continuous broadcasters, and can therefore be identified and tracked. In order to prevent tracking, easy to operate opt-out options ensuring the service set identifier (SSID) of the on-board Wi-Fi network is not collected should therefore be put in place by the vehicle and equipment manufacturers.

## 3 CASE STUDIES

103. This section addresses five specific examples of processing in the context of connected vehicles, which correspond to scenarios likely to be encountered by stakeholders in the sector. The examples cover data processing that requires calculating power which cannot be mobilised locally in the vehicle, and/or the sending of personal data to a third party to carry out further analysis or to provide further functionality remotely. For each type of processing, this document specifies the intended purposes, the categories of data collected, the retention period of such data, the rights of data subjects, the security measures to be implemented, and the recipients of the information. In the case some of these fields are not described in the following, the general recommendations described in the previous part apply.
104. The examples chosen are non-exhaustive and are meant to be indicative of the variety of types of processing, legal bases, actors, etc. that might be engaged in the context of connected vehicles.

### 3.1 Provision of a service by a third party

105. Data subjects may contract with a service provider in order to obtain added-value services relating to their vehicle. For example, a data subject may enter into a usage-based insurance contract that offers reduced insurance premiums for less driving ("Pay As You Drive") or good driving behaviour ("Pay How You Drive") and which necessitates monitoring of driving habits by the insurance company. A data subject could also contract with a company that offers roadside assistance in the event of a breakdown and which entails the transmission of the vehicle's location to the company or with a service provider in order to receive

messages or alerts relating to the vehicle's functioning (e.g., an alert on the state of brake wear, or a reminder of the technical-inspection date).

### 3.1.1 Usage-based insurance

106. "Pay as you drive" is a type of usage-based insurance that tracks the driver's mileage and/or driving habits to differentiate and reward "safe" drivers by giving them lower premiums. The insurer will require the driver to install a built-in telematics service, a mobile application or activate a built-in module from manufacturing that tracks the miles covered and/or the driving behaviour (braking pattern, rapid acceleration, etc.) of the policy holder. The information gathered by the telematic device will be used to assign the driver scores in order to analyse what risks he/she may pose to the insurance company.
107. As usage-based insurance requires consent under art. 5(3) of the ePrivacy directive, the EDPB outlines that the policy holder must have the choice to subscribe to a non-usage-based insurance policy. Otherwise, consent would not be considered freely given, as the performance of the contract would be conditional on the consent. Further, art. 7(3) GDPR requires that a data subject must have the right to withdraw consent.

#### 3.1.1.1 Legal basis

108. When the data is collected through a publicly available electronic communication service (for example *via* the SIM card contained in the telematics device), consent will be needed in order to gain access to information that is already stored in the vehicle as provided by art. 5(3) ePrivacy directive. Indeed, none of the exemptions provided by those provisions can apply in this context: the processing is not for the sole purpose of carrying out the transmission of a communication over an electronic communications network nor does it relate to an information society service explicitly requested by the subscriber or user. Consent could be collected at the time of the conclusion of the contract.
109. As regards the processing of personal data following the storage or access to the end-user's terminal equipment, the insurance company can rely on art. 6(1)(b) GDPR in this specific context provided it can establish both that the processing takes place in the context of a valid contract with the data subject and that processing is necessary in order that the particular contract with the data subject can be performed. Insofar as the processing is objectively necessary for the performance of the contract with the data subject, the EDPB considers that reliance upon art. 6(1)(b) GDPR would not have the effect of lowering the additional protection provided by art. 5(3) of the ePrivacy directive in this specific instance. That legal basis is materialised by the data subject signing a contract with the insurance company.

#### 3.1.1.2 Data collected

110. There are two types of personal data to be considered:
  - Z **commercial and transactional data:** data subject's identifying information, transaction-related data, data relating to means of payment, etc.;
  - Z **usage data:** personal data generated by the vehicle, driving habits, location, etc.
111. The EDPB recommends that, as far as possible, and given that there is a risk that the data collected via the telematics-box could be misused to create a precise profile of the driver's movements, raw data regarding driving behaviour should be either processed:

- Z inside the vehicle in telematics boxes or in the user's smartphone so that the insurer only accesses the results data (e.g., a score relating to driving habits), not detailed raw data (see section 2.1);
  - Z or by the telematics service provider on behalf of the controller (the insurance company) to generate numerical scores that are transferred to the insurance company on a defined basis. In this case, raw data and data directly relating to the identity of the driver must be separated. This means that the telematics service provider receives the real-time data, but does not know the names, licence plates, etc. of the policy holders. On the other hand, the insurer knows the names of policyholders, but only receives the scores and the total kilometres and not the raw data used to produce such scores.
112. Moreover, it has to be noted that if only the mileage is necessary for the performance of the contract, location data shall not be collected.

#### *3.1.1.3 Retention period*

113. In the context of data processing taking place for the performance of a contract (i.e. provision of a service), it is important to distinguish between two types of data before defining their respective retention periods:
- Z **commercial and transactional data:** those data can be retained in an active database for the full duration of the contract. At the end of the contract, they can be archived physically (on a separate medium: DVD, etc.) or logically (by authorisation management) in the event of possible litigation. Thereafter, at the end of the statutory limitation periods, the data shall be deleted or anonymised;
  - Z **usage data:** usage data can be classified as raw data and aggregated data. As stated above, if possible, data controllers or processors should not process raw data. If it is necessary, raw data should be kept only as long as they are required to elaborate the aggregated data and to check the validity of that aggregation process. Aggregated data should be kept as long as it is necessary for the provision of the service or otherwise requested by a Union or Member State law.

#### *3.1.1.4 Information and rights of data subjects*

114. Prior to the processing of personal data, the data subject shall be informed according to art. 13 GDPR, in a transparent and understandable way. In particular, he or she must be informed of the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period. In this last case, the EDPB recommends to adopt a pedagogic approach to emphasize the difference between raw data and the score produced on this basis, stressing, when it is the case, that the insurer will only collect the result of the score where appropriate.
115. Where data are not processed inside the vehicle but by a telematics provider on behalf of the controller (the insurance company), the information could usefully mention that, in this case, the provider will not have access to data directly relating to the identity of the driver (such as names, licence plates, etc.). Also, considering the importance of informing data subjects as to the consequences of processing of their personal data and the fact that data subjects should not be taken by surprise by the processing of their personal data, the EDPB recommends that data subject should be informed of the existence of profiling and the consequences of such profiling even if it does not involve any automated decision-making as referred to in art. 22 GDPR.

116. Regarding the right of data subjects, they shall be specifically informed of the available means to exercise his or her right of access, rectification, restriction and erasure. Since raw data collected in this context are provided by the data subject (through specific forms or through his or her activity) and processed on the basis of art. 6(1)(b) GDPR (performance of a contract), the data subject is entitled to exercise his or her right to data portability. As emphasized in the guidelines on the right to data portability, the EDPB strongly recommends “that data controllers clearly explain the difference between the types of data that a data subject can receive through the rights of subject access and data portability”.<sup>48</sup>

117. The information can be provided when the contract is signed.

#### *3.1.1.5 Recipient:*

118. The EDPB recommends that, as far as possible, the vehicle’s usage data should be processed directly in telematics boxes, so that the insurer only accesses the results data (e.g. a score), not detailed raw data.
119. If a telematics service provider collects the data on behalf of the controller (the insurance company) to generate numerical scores, it does not need to know the identity of the driver (such as names, licence plates, etc.) of the policy holders.

#### *3.1.1.6 Security:*

120. General recommendations apply. See section 2.7.

### **3.1.2 Renting and booking a parking space**

121. The owner of a parking place may want to rent it. For this, he/she lists a spot and sets a price for it on a web application. Then, once the parking spot is listed, the application notifies the owner when a driver wants to book it. The driver can select a destination and check for available parking spots based on multiple criteria. After the approval of the owner, the transaction is confirmed and the service provider handles the payment transaction then uses navigation to drive to the location.

#### *3.1.2.1 Legal basis*

122. When the data is collected through a publicly available electronic communication, art. 5(3) of the ePrivacy directive applies.
123. Because this is an information society service, art. 5(3) of the ePrivacy directive does not require consent for gaining access to information that is already stored in the vehicle when such a service is explicitly requested by the subscriber.
124. For the processing of personal data and only for data necessary for the performance of the contract to which the data subject is party, art. 6(1)(b) GDPR will be the legal basis.

#### *3.1.2.2 Data collected*

125. Data processed includes the driver contact details (name, email, telephone number, vehicle type (e.g. car, truck, motorcycle), license plate number, parking period, payment details (e.g. credit card info) as well as navigation data.

---

<sup>48</sup> Article 29 Working Party, Guidelines on the right to data portability under Regulation 2016/676, WP242 rev.01, endorsed by EDPB, p. 13.

### 3.1.2.3 *Retention period*

126. Data should be retained only as long as it is necessary to fulfil the parking contract or otherwise as provided by Union or Member State law. After that data is either anonymised or deleted.

### 3.1.2.4 *Information and rights of data subjects*

127. Prior to the processing of personal data, the data subject should be informed according to art. 13 GDPR, in a transparent and understandable way.
128. The data subject should be specifically informed of the available means to exercise his or her right of access, rectification, restriction and erasure. Since the data collected in this context are provided by the data subject (through specific forms or through his or her activity) and processed on the basis of art. 6(1)(b) GDPR (performance of a contract), the data subject is entitled to exercise his or her right to data portability. As emphasized in the guidelines on the right to data portability, the EDPB strongly recommends "*that data controllers clearly explain the difference between the types of data that a data subject can receive through the rights of subject access and data portability*".

### 3.1.2.5 *Recipient:*

129. In principle, only the data controller and the data processor have access to the data.

### 3.1.2.6 *Security:*

130. General recommendations apply. See section 2.7.

## 3.2 eCall

131. In the event of a serious accident in the European Union, the vehicle automatically triggers an eCall to 112, the EU-wide emergency number (see section 1.1 for further details) which allows an ambulance to be sent the place of the accident promptly according to Regulation (EU) 2015/758 of 29 April 2015 concerning type-approval requirements for the deployment of the eCall in-vehicle system based on the 112 service, and amending Directive 2007/46/EC (hereinafter - "Regulation (EU) 2015/758").
132. Indeed, the eCall generator installed inside the vehicle, which enables transmission via a public mobile wireless communications network initiates an emergency call, which is either triggered automatically by vehicle sensors or manually by the vehicle occupants only in the event of an accident. In addition to activation of the audio channel, the second event triggered automatically as a result of an accident consists in generating the Minimum Set of Data (MSD) and sending it to the public safety answering point (PSAP).

### 3.2.1 *Legal basis*

133. Regarding the application of the ePrivacy directive, two provisions have to be considered:
  - Z art. 9 regarding location data other than traffic data which only applies to electronic communication services;
  - Z art. 5(3) for the gaining access to information stored in the generator installed inside the vehicle.
134. Despite the fact that, in principle, those provisions require the consent of the data subject, Regulation (EU) 2015/758 constitutes a legal obligation to which the data controller is subject (the data subject has no genuine or free choice and will be unable to refuse the

processing of his/her data). Hence, Regulation (EU) 2015/758 overrides the need of the driver's consent for the processing of location data and the MSD.<sup>49</sup>

135. The legal basis of the processing of those data will be compliance with a legal obligation as provided for in art. 6(1)(c) GDPR (i.e., Regulation (EU) 2015/758).

### 3.2.2 Data collected

136. Regulation (EU) 2015/578 provides that data sent by the 112-based eCall in-vehicle system shall include only the minimum information as referred to in the standard EN 15722:2015 'Intelligent transport systems — eSafety — eCall minimum set of data (MSD)' including:

- Z the indication if eCall has been manually or automatically triggered;
- Z the vehicle type;
- Z the vehicle identification number (VIN);
- Z the propulsion type of the vehicle;
- Z the timestamp of the initial data message generation within the current eCall incident event;
- Z the last known vehicle latitude and longitude position determined at the latest moment possible before message generation;
- Z the vehicle's last known real direction of travel determined at the latest moment possible before message generation (only the last three locations of the vehicle).

### 3.2.3 Retention period

137. Regulation (EU) 2015/758 stipulates that data shall not be retained for longer than is needed for processing emergency situations. Those data shall be completely deleted when they are no longer needed for that purpose. Furthermore, in the internal memory of the eCall system, data shall be automatically and constantly deleted. Only the vehicle's last three positions can be stored, insofar as it is strictly necessary to specify the current position of the vehicle and the direction of travel at the time of the event.

### 3.2.4 Information and rights of data subjects

138. Art. 6 of the Regulation (EU) 2015/758 stipulates that manufacturers shall provide clear and complete information on data processing done using the eCall system. This information shall be provided in the owner's manual separately for the 112-based eCall in-vehicle system and any third-party service supported eCall systems prior to the use of the system. It includes:

- Z the reference to the legal basis for the processing;
- Z the fact that the 112-based eCall in-vehicle system is activated by default;
- Z the arrangements for data processing that the 112-based eCall in-vehicle system performs;

---

<sup>49</sup> It has to be noted that Article 8-1-f of the Council negotiation mandate for the proposal for an "ePrivacy" regulation does provide a specific exemption for eCall as consent is not needed when "*it is necessary to locate terminal equipment when an end-user makes an emergency communication either to the single European emergency number '112' or a national emergency number, in accordance with Article 13(3)*."

- ☐ the specific purpose of the eCall processing, which shall be limited to the emergency situations referred to in the first subparagraph of Art. 5(2) Regulation (EU) 2015/758;
- ☐ the types of data collected and processed and the recipients of that data;
- ☐ the time limit for the retention of data in the 112-based eCall in-vehicle system;
- ☐ the fact that there is no constant tracking of the vehicle;
- ☐ the arrangements for exercising data subjects' rights as well as the contact service responsible for handling access requests;
- ☐ any necessary additional information regarding traceability, tracking and processing of personal data in relation to the provision of a third-party service (TPS) eCall and/or other added value services, which shall be subject to explicit consent by the owner and in compliance with the GDPR. Particular account shall be taken of the fact that differences may exist between the data processing carried out through the 112-based eCall in-vehicle system and the TPS eCall in-vehicle systems or other added value services.

139. Furthermore, the service provider shall also provide the data subjects with information in accordance with art. 13 GDPR in a transparent and understandable way. In particular, he or she must be informed of the purposes of the processing for which the personal data are intended as well as the fact that the processing of personal data is based on a legal obligation to which the controller is subject.
140. In addition, taking into account the nature of the processing, the information about the recipients or categories of recipients of the personal data should be clear and the data subjects should be informed that the data are not be available outside the 112-based eCall in-vehicle system to any entities before the eCall is triggered.
141. Regarding rights of data subjects, it has to be noted that since the processing is based on a legal obligation, the right to object and the right to portability will not apply.

### 3.2.5 Recipient:

142. The data shall not be available outside the 112-based eCall in-vehicle system to any entities before the eCall is triggered.
143. When it is triggered (either manually by vehicle occupants or automatically as soon as an in-vehicle sensor detects a serious collision), the eCall system establishes a voice connection with the relevant PSAP and the MSD is sent to the PSAP operator.
144. Furthermore, data transmitted via the 112-based eCall in-vehicle system and processed by the PSAPs can be transferred to the emergency service and service partners referred to in Decision No 585/2014/EU only in the event of incidents related to eCalls and under the conditions set out in that Decision and are used exclusively for the attainment of the objectives of that Decision. Data processed by the PSAPs through the 112-based eCall in-vehicle system are not transferred to any other third parties without the explicit prior consent of the data subject.

### 3.2.6 Security

145. Regulation (EU) 2015/758 stipulates the requirements to incorporate into the eCall system technologies that strengthen the protection of privacy, in order to offer users the appropriate level of protection of privacy, as well as the guarantees needed to prevent

surveillance and abusive uses. In addition, manufacturers should ensure that the eCall system based on the number 112, as well as any other system providing an eCall that is handled by third-party services or an added-value service, are so designed that it is impossible for personal data to be exchanged between those systems.

146. Regarding PSAPs, Member States should ensure that personal data are protected against misuse, including unlawful access, alteration or loss, and that protocols concerning personal data storage, retention duration, processing and protection are established at the appropriate level and properly observed.

### 3.3 Accidentology studies

147. Data subjects may voluntarily agree to take part in accidentology studies aimed at better understanding the causes of road accidents and more generally scientific purposes.

#### 3.3.1 Legal basis

148. When the data are collected through a public electronic communication service, the data controller will have to collect the consent of the data subject for the gaining of access to information that is already stored in the vehicle as provided by art. 5(3) of the ePrivacy directive. Indeed, none of the exemptions provided by those provisions can apply in this context: the processing is not for the sole purpose of carrying out the transmission of a communication over an electronic communications network nor does it relate to an information society service explicitly requested by the subscriber or user.
149. Regarding the processing of personal data and taking into account the variety and amount of personal data needed for accidentology studies, the EDPB recommends the processing to be based on the prior consent of the data subject according to art. 6 GDPR. Such prior consent must be provided on a specific form, through which the data subject volunteers to take part to the study and have his or her personal data processed for that purpose. Consent shall be an expression of the free, specific, and informed will of the person whose data are being processed (e.g., ticking a box that is not pre-ticked, or configuring the onboard computer to activate a function in the vehicle). Such consent must be provided separately, for specific purposes, may not be bundled with the contract to buy or lease a new car and the consent must be as easily withdrawn as it is given. Withdrawal of consent shall lead to the processing being stopped. The data shall then be deleted from the active database, or anonymised.
150. Consent required by art. 5(3) of the ePrivacy directive and consent needed as a legal basis for the processing of data can be collected at the same time (for example by checking a box clearly indicating what the data subject is consenting to).
151. It has to be noted that, depending on the conditions of the processing (nature of the data controller, etc.), another legal basis can be lawfully chosen as long as it does not lower the additional protection provided by art. 5(3) ePrivacy directive (see paragraph 15). If the processing is based on another legal basis such as the performance of a task carried out in the public interest (art. 6(1)(e) GDPR), the EDPB recommends that the data subjects are included in the study on a voluntary basis.

#### 3.3.2 Data collected

152. The data controller shall only collect personal data that are strictly necessary for the processing.

153. There are two types of data to be considered:

- Z **data relating to participants and vehicles** ;
- Z **technical data from vehicles** (instantaneous speed, etc.).

154. Scientific research linked to accidentology justifies the collection of the instantaneous speed, including by legal persons who do not administer a public service in the strict sense.

155. Indeed, as noted above, the EDPB considers that instantaneous speed collected in the context of an accidentology study is not offence-related data by destination (i.e., it is not being collected for the purpose of investigating or prosecuting an offence), which justifies its collection by legal persons who do not administer a public service in the strict sense.

### 3.3.3 Retention period

156. It is important to distinguish between two types of data. First, the data relating to participants and vehicles can be retained for the duration of the study. Second, the technical data from vehicles should be retained for as short as possible for the purpose. In this regard, five years from the end date of the study appears to be a reasonable period. At the end of that period, the data shall be deleted or anonymised.

### 3.3.4 Information and rights of data subjects

157. Prior to the processing of personal data, the data subject shall be informed according to art. 13 GDPR, in a transparent and understandable way. In particular, in the case of collecting instantaneous speed, the data subjects should be specifically informed of the data collection. Since the data processing is based on consent, the data subject must be specifically informed of the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal. Moreover, because the data collected in this context are provided by the data subject (through specific forms or through his or her activity) and processed on the basis of art. 6(1)(a) GDPR (consent), the data subject is entitled to exercise his or her right to data portability. As emphasized in the guidelines on the right to data portability, the EDPB strongly recommends "that data controllers clearly explain the difference between the types of data that a data subject can receive through the rights of subject access and data portability". Consequently, the data controller should provide an easy way to withdraw his consent, freely and at any time, as well as develop tools to be able to answer data portability requests.

158. That information can be given upon signing the form to agree to take part in the accidentology study.

### 3.3.5 Recipient

159. In principle, only the data controller and the data processor have access to the data.

### 3.3.6 Security

160. As noted above, the security measures put in place shall be adapted to the level of data sensitivity. For instance, if instantaneous speed (or any other data related to criminal convictions and offences) is collected as part of the accidentology study, the EDPB strongly recommends putting in place strong security measures, such as:

- Z implementing pseudonymisation measures (e.g., secret-key hashing of data like the surname/first name of the data subject and the serial number);

- ☐ storing data relating to instantaneous speed and to location in separate databases (e.g., using a state-of-the-art encryption mechanism with distinct keys and approval mechanisms);
- ☐ and/or deleting location data as soon as the reference event or sequence is qualified (e.g., the type of road, day/night), and the storage of directly-identifying data in a separate database that can only be accessed by a small number of people.

### 3.4 Tackle auto theft

161. Data subjects may wish, in the case of theft, to attempt to find their vehicle using location. Using location data is limited to the strict needs of the investigation and to the case assessment by the competent legal authorities.
162. When the data is collected through a publicly available electronic communication service, art. 5(3) of the ePrivacy directive applies.
163. Because this is an information society service, art. 5(3) of the ePrivacy directive does not require consent for gaining access to information that is already stored in the vehicle when such a service is explicitly requested by the subscriber.
164. Regarding the processing of personal data, the legal basis for processing the location data will be the consent of the vehicle's owner, or, if applicable, the performance of a contract (only for data necessary for the performance of the contract to which the vehicle's owner is party).
165. Consent shall be an expression of the free, specific, and informed will of the person whose data are being processed (e.g. ticking a box that is not pre-ticked, or configuring the on-board computer to activate a function in the vehicle). Freedom to give consent involves the option of withdrawing consent at any time, of which the data subject should be expressly informed. Withdrawal of consent shall lead to the processing being stopped. The data should then be deleted from the active database, anonymised, or archived.

#### 3.4.2 Data collected

166. Location data can only be transmitted as of the declaration of theft, and cannot be collected continuously the rest of the time.

#### 3.4.3 Retention period

167. Location data can only be retained for the period during which the case is assessed by the competent legal authorities, or until the end of a procedure to dispel doubt that does not end with confirmation of the theft of the vehicle.

#### 3.4.4 Information of the data subjects

168. Prior to the processing of personal data, the data subject should be informed according to art. 13 GDPR, in a transparent and understandable way. More specifically, the EDPB recommends that the data controller emphasizes that there is no constant tracking of the vehicle and that location data can only be collected and transmitted as of the declaration of theft. Moreover, the controller must provide the data subject with information relating to the fact that only approved officers of the remote-surveillance platform and legally approved authorities have access to the data.
169. Regarding the rights of the data subjects, when the data processing is based on consent, the data subject should be specifically informed of the existence of the right to withdraw

consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal. Besides, when the data collected in this context are provided by them (through specific forms or through his or her activity) and processed on the basis of art. 6(1)(a) (consent) or art. 6(1)(b) GDPR (performance of a contract), the data subject is entitled to exercise his or her right to data portability. As emphasized in the guidelines on the right to data portability, the EDPB strongly recommends “that data controllers clearly explain the difference between the types of data that a data subject can receive through the rights of subject access and data portability”.

170. Consequently, the data controller should provide an easy way to withdraw his consent (only when consent is the legal basis), freely and at any time, as well as develop tools to be able to answer data portability requests.
171. The information can be provided when the contract is signed.

#### 3.4.5 Recipients

172. In the event of a theft declaration, location data can be passed on the (i) approved officers of the remote-surveillance platform, and (ii) to the legally approved authorities.

#### 3.4.6 Security

173. General recommendations apply. See section 2.7

# Guidelines



**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**

**Version 2.0**

**Adopted on 15 December 2020**

## Version history

Version 2.0	15 December 2020	Adoption of the Guidelines after public consultation
Version 1.0	18 February 2020	Adoption of the Guidelines for public consultation

## Table of contents

1	General .....	5
1.1	Purpose .....	5
1.2	General rules applicable to international transfers.....	6
1.3	Definition of a public authority or body .....	6
2	General Recommendations for the Appropriate Safeguards under both articles 46 (2) (a) and 46 (3) (b) GDPR .....	7
2.1	Purpose and scope.....	8
2.2	Definitions.....	8
2.3	Data protection principles .....	8
2.3.1	Purpose limitation principle .....	8
2.3.2	Data accuracy and minimisation principles.....	8
2.3.3	Storage limitation principle .....	9
2.3.4	Security and confidentiality of data .....	9
2.4	Rights of the data subjects.....	9
2.4.1	Right to Transparency .....	10
2.4.2	Rights of access, to rectification, erasure, restriction of processing and to object .....	10
2.4.3	Automated individual decision-making.....	11
2.4.4	Right to Redress.....	11
2.4.5	Restrictions to the Rights of the data subjects.....	11
2.5	Restrictions on onward transfers and sharing of data (including disclosure and government access).....	12
2.6	Sensitive data.....	13
2.7	Redress mechanisms.....	13
2.8	Supervision mechanisms.....	15
2.9	Termination clause .....	16
3	Specific information on article 46 GDPR .....	17
3.1	Specific information on legally binding and enforceable instruments - Article 46 (2) (a) GDPR.....	17
3.2	Specific information on administrative arrangements - Article 46 (3) (b) GDPR.....	17
4	Procedural questions .....	19

## **The European Data Protection Board**

Having regard to Article 70 (1e) 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<sup>1</sup>,

Having regard to Article 12 and Article 22 of its Rules of Procedure,

### **HAS ADOPTED THE FOLLOWING GUIDELINES**

---

<sup>1</sup> References to “Member States” made throughout these guidelines should be understood as references to “EEA Member States”.

# 1 GENERAL

## 1.1 Purpose

1. This document seeks to provide guidance as to the application of Articles 46 (2) (a) and 46 (3) (b) of the General Data Protection Regulation (GDPR) on transfers of personal data from EEA public authorities or bodies (hereafter “public bodies”) to public bodies in third countries or to international organisations, to the extent that these are not covered by an adequacy finding adopted by the European Commission<sup>2</sup>. Public bodies may choose to use these mechanisms, which the GDPR considers more appropriate to their situation, but are also free to rely on other relevant tools providing for appropriate safeguards in accordance with Article 46 GDPR.
2. The guidelines are intended to give an indication as to the expectations of the European Data Protection Board (EDPB) on the safeguards required to be put in place by a legally binding and enforceable instrument between public bodies pursuant to Article 46 (2) (a) GDPR or, subject to authorisation from the competent supervisory authority (SA), by provisions to be inserted into administrative arrangements between public bodies pursuant to Article 46 (3) (b) GDPR.<sup>3</sup> The EDPB strongly recommends parties to use the guidelines as a reference at an early stage when envisaging concluding or amending such instruments or arrangements.<sup>4</sup>
3. The guidelines are to be read in conjunction with other previous work done by the EDPB (including endorsed documents by its predecessor, the Article 29 Working Party<sup>5</sup> (“WP29”)) on the central questions of territorial scope and transfers of personal data to third countries<sup>6</sup>. The guidelines will be reviewed and if necessary updated, based on the practical experience gained from the application of the GDPR.
4. The present guidelines cover international data transfers between public bodies occurring for various administrative cooperation purposes falling within the scope of the GDPR. As a consequence and in accordance with Article 2 (2) of the GDPR, they do not cover transfers in the area of public security, defence or state security. In addition, they do not deal with data processing and transfers by competent authorities for criminal law enforcement purposes, since this is governed by a separate specific instrument, the law enforcement Directive<sup>7</sup>. Finally, the guidelines only focus on transfers between public bodies and do not cover transfers of personal data from a public body to a private entity or from a private entity to a public body.

---

<sup>2</sup> For example Japanese public bodies, which are not covered by the Japan Adequacy Decision as it only covers private sector organisations.

<sup>3</sup> These guidelines use the term "international agreements" to refer to legally binding and enforceable instruments pursuant to Article 46(2)(a) GDPR and to administrative arrangements pursuant to Article 46(3)(b) GDPR.

<sup>4</sup> Art. 96 GDPR states that agreements that were concluded prior to 24 May 2016 shall remain in force until amended, replaced or revoked.

<sup>5</sup> The Working Party of EU Data Protection Authorities established under Article 29 of the Data Protection Directive 95/46/EC.

<sup>6</sup> See Article 29 Working Party, Adequacy Referential (WP254 rev.01, endorsed by the EDPB on 25 May 2018), EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 and EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3).

<sup>7</sup> Directive (EU) 2016/680 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.

## 1.2 General rules applicable to international transfers

5. According to Article 44 of the GDPR the data exporter transferring personal data to third countries or international organisations must, in addition to complying with Chapter V of the GDPR, also meet the conditions of the other provisions of the GDPR. In particular, each processing activity must comply with the data protection principles in Article 5 GDPR, be lawful in accordance with Article 6 GDPR and comply with Article 9 GDPR in case of special categories of data. Hence, a two-step test must be applied: first, a legal basis must apply to the data processing as such together with all relevant provisions of the GDPR; and as a second step, the provisions of Chapter V of the GDPR must be complied with.
6. The GDPR specifies in its Article 46 that "*in the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available*". Such appropriate safeguards may be provided for by a legally binding and enforceable instrument between public bodies (Article 46 (2) (a) GDPR) or, subject to authorisation from the competent SA, by provisions to be inserted into administrative arrangements between public bodies which include enforceable and effective data subject rights (Article 46 (3) (b) GDPR). As clarified by the Court of Justice of the European Union (CJEU), such appropriate safeguards must be capable of ensuring that data subjects whose personal data are transferred are afforded a level of protection essentially equivalent to that which is guaranteed within the EEA.<sup>8</sup>
7. Aside from this solution and in its absence, Article 49 of the GDPR also offers a limited number of specific situations in which international data transfers may take place when there is no adequacy finding by the European Commission<sup>9</sup>. In particular, one exemption covers transfers necessary for important reasons of public interest recognised in Union law or in the law of the Member State to which the controller is subject, including in the spirit of reciprocity of international cooperation<sup>10</sup>. However, as explained in previous guidance issued by the EDPB, the derogations provided by Article 49 GDPR must be interpreted restrictively and mainly relate to processing activities that are occasional and non-repetitive<sup>11</sup>.

## 1.3 Definition of a public authority or body

8. The GDPR does not define what constitutes a 'public authority or body'. The EDPB considers that this notion is broad enough to cover both public bodies in third countries and international organisations.<sup>12</sup> With respect to public bodies in third countries, the notion is to be determined under domestic law. Accordingly, public bodies include government authorities at different levels (e.g. national, regional and local authorities), but may also include other bodies governed by public law (e.g. executive agencies, universities, hospitals, etc.).<sup>13</sup> In accordance with Article 4 (26) GDPR, 'international

---

<sup>8</sup> Court of Justice of the European Union, Case C-311/18, Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems ("Schrems II"), para. 96.

<sup>9</sup> For further information on Article 49 and its interplay with Article 46 in general, please see EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679.

<sup>10</sup> See EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, page 10.

<sup>11</sup> See EDPB Guidelines on derogations of Article 49 under Regulation 2016/679, page 5.

<sup>12</sup> See also recital 108 of the GDPR.

<sup>13</sup> See, e.g. the definition of 'public sector body' and 'body governed by public law' in Article 2 (1) and (2) of Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public-sector information (OJ L 345, 31.12.2003, page 90).

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

9. The EDPB recalls that the application of the GDPR is without prejudice to the provisions of international law, such as the ones governing the privileges and immunities of international organisations. At the same time, it is important to recall that any EEA public body transferring data to international organisations has to comply with the GDPR rules on transfers to third countries or international organisations.<sup>14</sup>

## 2 GENERAL RECOMMENDATIONS FOR THE APPROPRIATE SAFEGUARDS UNDER BOTH ARTICLES 46 (2) (a) AND 46 (3) (b) GDPR

10. Unlike Article 26 (2) of the 95/46/EC Directive, Article 46 of the GDPR provides for additional appropriate safeguards as tools for transfers between public bodies:
  - (i) a legally binding and enforceable instrument, Article 46 (2) (a) GDPR or
  - (ii) provisions to be inserted into administrative arrangements, Article 46 (3) (b) GDPR.

These instruments and arrangements may be of bilateral or multilateral nature.

11. The following section provides some general recommendations to help ensure that legally binding instruments or administrative arrangements (hereinafter "international agreements") between public bodies are in compliance with the GDPR.
12. Although Article 46 and recital 108 of the GDPR do not provide specific indications on the guarantees to be included in such international agreements, taking into account Article 44 of the GDPR<sup>15</sup> and the recent CJEU case law<sup>16</sup> the EDPB hereby has elaborated a list of minimum safeguards to be included in international agreements between public bodies falling under Articles 46 (2) (a) or 46 (3) (b) GDPR. These safeguards aim to ensure that the level of protection of natural persons under the GDPR is not undermined when their personal data is transferred outside of the EEA and that data subjects are afforded a level of protection essentially equivalent to that guaranteed within the EU by the GDPR.<sup>17</sup>
13. In accordance with the recent CJEU case law<sup>18</sup>, it is the responsibility of the transferring public body in a Member State, if needed with the help of the receiving public body, to assess whether the level of protection required by EU law is respected in the third country, in order to determine whether the list of safeguards included in the international agreement can be complied with in practice, taking into account the possible interference created by the third country legislation with compliance with these safeguards.

---

<sup>14</sup> See EDPB Guidelines 3/2018 on the territorial scope of the GDPR, p. 23.

<sup>15</sup> Article 44 of the GDPR states: "*All provisions of this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.*"

<sup>16</sup> CJEU, July 16, 2020, Judgment in case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems ("Schrems II").

<sup>17</sup> CJEU, July 16, 2020, Judgment in case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems ("Schrems II"), para 105.

<sup>18</sup> Idem.

14. In this respect, it should also be noted that, to ensure the safeguards listed in these guidelines, international agreements can build on already existing elements in the national law of a third country or the internal rules/regulatory framework of an international organisation.

## 2.1 Purpose and scope

15. International agreements should define their scope and their purposes should be explicitly and specifically determined. In addition, they should clearly state the categories of personal data affected and the type of processing of the personal data which is transferred and processed under the agreement.

## 2.2 Definitions

16. International agreements should contain definitions of the basic personal data concepts and rights in line with the GDPR relevant to the agreement in question. By way of example, such agreements should, if referenced, include the following important definitions: “personal data”, “processing of personal data”, “data controller”, “data processor”, “recipient” and “sensitive data”.

## 2.3 Data protection principles

17. International agreements shall contain specific wording requiring that the core data protection principles are ensured by both parties.

### 2.3.1 Purpose limitation principle

18. International agreements need to specify the purposes for which personal data is to be transferred and processed including compatible purposes for further processing, as well as to ensure that the data will not be further processed for incompatible purposes. Compatible purposes may include storing for archiving purposes in the public interest, as well as processing for scientific or historical research purposes or statistical purposes. It is recommended, for better clarity, that the specific purposes for the processing and transferring of the data are listed in the international agreement itself.

19. To avoid any risk of a “function creep”, such agreements should also specify that transferred data cannot be used for any purpose other than those expressly mentioned in the agreement, except as set out in the paragraph below.

20. If both parties to the international agreement wish to allow the receiving public body to make another compatible use of the transmitted personal data, further use by the receiving public body shall only be permitted if compatible with the original one and previously notified to the transferring public body which may oppose for specific reasons.

### 2.3.2 Data accuracy and minimisation principles

21. The international agreement must specify that the data transferred and further processed must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are transmitted and further processed.

22. In practice, this data minimisation principle is important to avoid the transfer of personal data when they are inadequate or excessive.

23. Moreover, data should be accurate and up to date, having regard to the purposes for which they are processed. An international agreement must therefore provide that the transferring party will ensure

that the personal data transferred under the agreement is accurate and, where applicable, up to date. In addition, the agreement should provide that, if one of the parties becomes aware that inaccurate or out of date data has been transmitted or is being processed, it must notify the other party without delay. Finally, the agreement should ensure that, where it is confirmed that data transmitted or being processed is inaccurate, each party processing the data shall take every reasonable step to rectify or erase the information.

### 2.3.3 Storage limitation principle

24. Parties must ensure that the international agreement contains a data retention clause. This clause should specify in particular that personal data shall not be retained indefinitely but shall be kept in a form which permits identification of data subjects only for the time necessary for the purpose for which it was transferred and subsequently processed. That may include storing it for as long as necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, provided that appropriate technical and organisational measures are put in place to safeguard the rights and freedoms of the data subjects, such as additional technical measures (e.g. security measures, pseudonymisation) and access restrictions. When a maximum retention period is not already set in national legislation or the internal rules/regulatory framework of an international organisation, a maximum retention period should be set in the text of the agreement.

### 2.3.4 Security and confidentiality of data

25. The parties should commit to ensure the security and the confidentiality of the personal data processing and transfers they carry out.  
In particular, the parties should commit to having in place appropriate technical and organisational measures to protect personal data against accidental or unlawful access, destruction, loss, alteration, or unauthorised disclosure. These measures may include, for example, encryption including in transit, pseudonymisation, marking information as personal data transferred from the EEA, 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.  
The level of security should take into consideration the risks, the state of the art and the related costs.
26. The international agreement may furthermore specify that, if one of the parties becomes aware of a personal data breach, it will inform the other party (ies) as soon as possible and use reasonable and appropriate means to remedy the personal data breach and minimise the potential adverse effects, including by communicating to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person.  
It is recommended that the notification timeline for a personal data breach as well as the procedures for communication to the data subject are defined in the international agreement.

### 2.4 Rights of the data subjects

27. The international agreement must ensure enforceable and effective data subject rights as specified in article 46 (1) and recital 108 of the GDPR.
28. The rights available to the data subjects, including the specific commitments taken by the parties to provide for such rights, should be listed in the agreement. To be effective, the international agreement must provide for mechanisms that ensure their application in practice. Moreover, any breach of data subject rights must carry an appropriate remedy.

#### 2.4.1 Right to Transparency

29. Parties must ensure that the international agreement contains clear wording describing the transparency obligations of the parties.
30. Such obligations should include on the one hand, a general information notice with, as a minimum, information on how and why the public bodies may process and transfer personal data, the relevant tool used for the transfer, the entities to which such data may be transferred, the rights available to data subjects and applicable restrictions, available redress mechanisms and contact details for submitting a dispute or claim.
31. However, it is important to recall that, for the transferring public body, a general information notice on the website of the public body concerned will not suffice. Individual information to data subjects should be made by the transferring public body in accordance with the notification requirements of Articles 13 and 14 GDPR<sup>19</sup>.  
The international agreement can also provide for some exceptions to such individual information. These exceptions are limited and should be in line with the ones provided under Article 14 (5) GDPR, for example where the data subject already has the information or where the provision of such information proves impossible or would involve a disproportionate effort.
32. The parties must commit to make the international agreement available to data subjects on request and to make the international agreement or the relevant provisions providing for appropriate safeguards publicly available on their website. To the extent necessary to protect sensitive or other confidential information, the text of the international agreement may be redacted prior to sharing a copy or making it publicly available. Where necessary to allow the data subject to understand the content of the international agreement, the parties must provide a meaningful summary thereof.

#### 2.4.2 Rights of access, to rectification, erasure, restriction of processing and to object

33. The international agreement should safeguard the data subject's right to obtain information about and access to all personal data relating to him/her that are processed, the right to rectification, erasure and restriction of processing and where relevant the right to oppose to the data processing on grounds relating to his or her particular situation.
34. As regards the right of access, the international agreement should specify that individuals shall have the right vis-à-vis the receiving public body to obtain confirmation as to whether or not personal data concerning him/her is being processed, and if that is the case, access to that data; as well as to specific information concerning the processing, including the purpose of the processing, the categories of personal data concerned, the recipients to whom personal data is disclosed, the envisaged storage period and redress possibilities.
35. The agreement should furthermore specify when these rights can be invoked and include the modalities on how the data subjects can exercise these rights before both parties as well as on how the parties will respond to such requests. For example, with respect to deletion, the international agreement could state that data is to be deleted when the information has been processed unlawfully or is no longer necessary for the purpose of processing. Moreover, the international agreement should stipulate that the parties will respond in a reasonable and timely manner to requests from data subjects. The international agreement could also state that the parties may take appropriate steps,

---

<sup>19</sup> See EDPB Guidelines on transparency under Regulation 2016/679, WP 260 rev.01, pages 13 to 22.

such as charging reasonable fees to cover administrative costs where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character.

36. The international agreement should also allot an obligation of the transferring public body to provide information to the data subject, once his/her personal data have been transferred, on the action taken on his/her request under the rights provided for by the international agreement without undue delay by setting an appropriate time limit (e.g. one month). Finally, information should be provided to the data subject, if the parties do not take action on the request of the data subject, without delay by setting an appropriate time limit (e.g. within one month of receipt of the request), of the reasons for not taking action and on the possibility of lodging a complaint and of seeking a judicial remedy.
37. The international agreement can also provide for exceptions to these rights. For example, exceptions to the right of access and deletion such as the ones provided under Article 15 (4) and 17 (3) GDPR could be provided. Similarly, exceptions to individual rights could be foreseen where personal data is processed for scientific or historical research purposes, statistical purposes, or archiving purposes, in so far as such rights would be likely to render impossible or seriously impair the achievement of these specific purposes, and provided that appropriate safeguards are put in place (e.g. technical and organisational measures, including pseudonymisation). Finally, the agreement may provide that the parties may decline to act on a request that is manifestly unfounded or excessive.

#### 2.4.3 Automated individual decision-making

38. If relevant to the agreement in question, international agreements should as a general principle contain a clause stating that the receiving public body will not take a decision based solely on automated individual decision-making, including profiling, producing legal effects concerning the data subject in question or similarly affecting this data subject. Where the purpose of the transfer includes the possibility for the receiving public body to take decisions solely on automated processing in the sense of Article 22 GDPR, this should only take place under certain conditions set forth in the international agreement, such as the need to obtain the explicit consent of the data subject. If the decision does not comply with such conditions, the data subject should have the right not to be subject to it. Where it allows automated individual decision-making, the international agreement 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 and obtain human intervention.

#### 2.4.4 Right to Redress

39. The safeguarded data subject rights have to be enforceable and effective. Therefore, the data subject must have access to redress. Different examples of ways to offer redress mechanisms are indicated below under sections 2.7 and 3.

#### 2.4.5 Restrictions to the Rights of the data subjects

40. The international agreement can also provide for restrictions to the rights of data subjects. These restrictions should be in line with the restrictions envisaged by Article 23 GDPR. Such a restriction has to be a necessary and proportionate measure in a democratic society to safeguard important objectives of public interest, in line with the ones listed in Article 23(1) GDPR, including the rights and freedom of others, national security, defence or the prevention, investigation, detection or prosecution of criminal offences. It needs to be provided by law or, in the case of international

organisations, the applicable internal rules/regulatory framework, and shall continue only for as long as the reason for the restriction continues to exist.

## 2.5 Restrictions on onward transfers and sharing of data (including disclosure and government access)

41. Onward transfers by the receiving public body or international organisation to recipients not bound by the agreement should, as a rule, be specifically excluded by the international agreement. Depending on the subject matter and the particular circumstances at hand, the parties may find it necessary to allow onward transfers. In this case, under the condition that the purpose limitation principle is respected<sup>20</sup>, the international agreement should foresee that such onward transfers can only take place if the transferring public body has given its prior and express authorisation and the receiving third parties commit to respect the same data protection principles and safeguards as included in the international agreement. This should include a commitment to provide to data subjects the same data protection rights and guarantees as provided in the international agreement in order to ensure that the level of protection will not be diminished if data are onward transferred.
42. As a rule, the same safeguards as for onward transfers should apply to sharing of personal data within the same country, i.e. the international agreement shall exclude this onward sharing and exemptions should in general only be allowed if the transferring public body has given its prior and express authorization and the receiving third parties commit to respect the same data protection principles and safeguards as included in the international agreement.
43. It is recommended that before requesting the express authorisation of the transferring public body the receiving public body or international organisation provides sufficient information on the type of personal data that it intends to transfer/share, the reasons and purposes for which it considers it to be necessary to transfer/share the personal data as well as, in case of onward transfers, the countries or international organisations to which it intends to onward transfer personal data so as to be able to assess the third country legislation or, in the case of international organisations, the applicable internal rules/regulatory framework.
44. In cases where it is necessary to allow sharing of personal data with a third party in the same country of the receiving public body or another international organisation, the sharing could be allowed in specific circumstances either with prior and express authorization of the transferring public body or as long as there is a binding commitment from the receiving third party to respect the principles and guarantees included in the international agreement.
45. In addition, the international agreement could specify exceptional circumstances in which onward sharing could take place without prior authorisation or the abovementioned commitments in line with the derogations listed in Article 49 of the GDPR, for example when this specific sharing would be necessary in order to protect the vital interests of the data subject or other persons or necessary for the establishment, exercise or defence of legal claims. Such exceptional circumstances could also arise if the onward sharing is required under the law of the receiving party, as necessary for directly related investigations/ court proceedings.
46. In the cases mentioned in the paragraph above, the international agreement should clearly state the specific and exceptional circumstances under which such data sharing is allowed. The receiving public body or international organisation should also be obliged to notify the transferring public body prior to the sharing and include information about the data shared, the receiving third party and the legal

---

<sup>20</sup> See above under 2.3.1.

basis for the sharing. In its turn the transferring public body should keep a record of such notifications from the receiving public body or international organisation and provide its SA with this information upon request. Where providing such notification prior to the sharing will impinge on confidentiality obligations provided for by law, e.g. to preserve the confidentiality of an investigation, the specific information should be provided as soon as possible after the sharing. In such a case, general information on the type of requests received over a specified period of time, including information about the categories of data requested, the requesting body and the legal basis for disclosure, should be provided to the transferring body at regular intervals.

47. In all of the above scenarios, the international agreement should only allow disclosures of personal data to other public authorities in the third country of the receiving public body that do not go beyond what is necessary and proportionate in a democratic society to safeguard important objectives of public interest in line with the ones listed in Article 23 (1) GDPR and in accordance with the jurisprudence of the CJEU. In order to assess a possible access by third country public authorities for surveillance purposes, the transferring public authority should take into account the elements recalled in the four European Essential Guarantees<sup>21</sup>. These include the availability of an effective remedy for data subjects in the third country of the receiving public body if their personal data is accessed by public authorities.<sup>22</sup> In case of transfers to international organisations, any such access must be in compliance with international law and without prejudice in particular to the privileges and immunities of the international organisation.
48. Depending on the case at hand, it may be useful to require to include an annex to the international agreement enumerating the laws governing onward sharing with other public bodies including for surveillance purposes in the destination country. Any changes to this annex should be notified to the transferring party within a set period of time.

## 2.6 Sensitive data

49. If an international agreement provides for the transfer of sensitive personal data within the meaning of Article 9 (1) of the GDPR, additional safeguards addressing the specific risks, to be implemented by the receiving public body or international organisation, should be included. These could, for example, include restrictions as access restrictions, restrictions of the purposes for which the information may be processed, restrictions on onward transfers, etc. or specific safeguards, e.g. additional security measures, requiring specialized training for staff allowed to access the information.

## 2.7 Redress mechanisms

50. In order to guarantee enforceable and effective data subjects rights the international agreement must provide for a system that enables data subjects to continue to benefit from redress mechanisms after their data has been transferred to a non EEA country or an international organisation. These redress mechanisms must provide recourse for individuals who are affected by non-compliance with the provisions of the chosen instrument and thus the possibility for data subjects whose personal data have been transferred from the EEA to lodge complaints regarding such non-compliance and to have these complaints resolved. In particular, the data subject must be ensured an effective route to complain to the public bodies that are parties to the international agreement and (either directly or

---

<sup>21</sup> See EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

<sup>22</sup> See EDPB Recommendations 02/2020, Guarantee D, p. 13 and seq.

after having addressed the relevant party) to an independent oversight mechanism. Moreover, a judicial remedy should, in principle, be available.

51. First, the receiving public body should commit to put in place a mechanism to effectively and timely handle and resolve complaints from data subjects concerning compliance with the agreed data protection safeguards. Moreover, data subjects should be provided with the possibility to obtain effective administrative redress before an independent oversight body, including, where available, an independent data protection authority<sup>23</sup>.
52. Second, the agreement should allow for a judicial remedy including compensation for damages - both material and non-material - as a result of the unlawful processing of the personal data. If there is no possibility to ensure effective judicial redress, for example due to restrictions in the domestic law or the specific status of the receiving public body, e.g. international organisations, the international agreement must provide for alternative safeguards. Those alternative safeguards must offer the data subject guarantees essentially equivalent to those required by Article 47 of the Charter of Fundamental Rights of the European Union (EU Charter)<sup>24</sup>.
53. In that case, the international agreement could create a structure which enables the data subject to enforce its rights outside the courts, for example through quasi-judicial, binding mechanisms such as arbitration or alternative dispute resolution mechanisms such as mediation, which would guarantee an independent review and bind the receiving public body<sup>25</sup>. Moreover, the public body transferring the personal data could commit to be liable for compensation of damages through unlawful processing of the personal data which are testified by the independent review.  
Exceptionally, other, equally independent and effective redress mechanisms could be put in place by the agreement, for instance effective redress mechanisms implemented by international organisations.
54. For all of the abovementioned redress mechanisms, the international agreement should contain an obligation for the parties to inform each other of the outcome of the proceedings, in particular if a complaint of an individual is dismissed or not resolved.
55. The redress mechanism must be combined with the possibility for the transferring public body to suspend or terminate the transfer of personal data under the international agreement where the parties do not succeed in resolving a dispute amicably until it considers that the issue has been satisfactorily addressed by the receiving public body. Such a suspension or termination, if carried out, must be accompanied by a commitment from the receiving public body to return or delete the personal data. The transferring public body must notify the suspension or termination to the competent national SA.

---

<sup>23</sup> See also section 2.8 on supervision mechanism.

<sup>24</sup> CJEU, July 16,2020, Judgment in case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems ("Schrems II"), paras 96, 186 and seq.

<sup>25</sup> CJEU, October 6, 2015, Judgment in case C-362/14, Maximillian Schrems v Data Protection Commissioner ("Schrems"), paras 41 and 95; ECJ July 16,2020, Judgment in case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems ("Schrems II"), paras 186,187,189, 195 and seq.

## 2.8 Supervision mechanisms

56. In order to make sure that all obligations created under the international agreement are fulfilled, the international agreement must provide for independent supervision monitoring the proper application of the agreement and interferences with the rights provided under the agreement.
57. First, the agreement should provide for internal supervision ensuring compliance with the agreement. Each party to the agreement should conduct periodic internal checks of the procedures put in place and of the effective application of the safeguards provided in the agreement. The periodic internal checks should also verify any changes in legislation that would prevent the party (ies) to comply with the data protection principles and safeguards included in the international agreement. Moreover, it could be provided that a party to the agreement can also request from another party to the agreement to conduct such a review. The international agreement must require that the parties must respond to inquiries from the other party concerning the effective implementation of the safeguards in the agreement. Each party conducting a review should communicate the results of the checks to the other party (ies) to the agreement. Ideally, such communication should also be made to the independent oversight mechanism governing the agreement.
58. In addition, the international agreement must include the obligation that a party informs the other party without delay if it is unable to effectively implement the safeguards in the agreement for any reason. For this case the international agreement must foresee the possibility for the transferring public body to suspend or terminate the transfer of personal data under the international agreement to the receiving public body until such time as the receiving public body informs the transferring public body that it is again able to act consistent with the safeguards. The transferring body must notify the change of situation as well as the suspension of transfers or termination of the agreement to the competent national SA.
59. Secondly, the agreement must provide for independent supervision in charge of ensuring that the parties comply with the provisions set out in the agreement. This follows directly from the EU Charter<sup>26</sup> and the European Convention of Human Rights (ECHR)<sup>27</sup> in accordance with the jurisprudence of the European Court of Human Rights (ECtHR) and in the terms established in primary law<sup>28</sup> as well as the corresponding case law.

---

<sup>26</sup> Articles 7, 8 and 47 of the EU Charter.

<sup>27</sup> Article 8 ECHR.

<sup>28</sup> Article 6 Lisbon Treaty

*"1. The Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, which shall have the same legal value as the Treaties.*

*The provisions of the Charter shall not extend in any way the competences of the Union as defined in the Treaties.*

*The rights, freedoms and principles in the Charter shall be interpreted in accordance with the general provisions in Title VII of the Charter governing its interpretation and application and with due regard to the explanations referred to in the Charter, that set out the sources of those provisions.*

*2. The Union shall accede to the European Convention for the Protection of Human Rights and Fundamental Freedoms. Such accession shall not affect the Union's competences as defined in the Treaties.*

*3. Fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union's law."*

- 60. The CJEU, has, since 2015<sup>29</sup>, reiterated the necessity of having an independent redress and supervision mechanism.<sup>30</sup> Likewise, the ECtHR has frequently highlighted in its rulings that any interference with the right to respect for private life as enshrined in Article 8 ECHR needs to be subject to an effective, independent and impartial oversight system<sup>31</sup>.
- 61. The agreement could, for example, invoke oversight by a competent supervisory authority, if there is one in the country of the public body receiving the EEA personal data, even if the GDPR does not specify that the competent supervisory authority needs to be the external oversight body. Moreover, the agreement could include the voluntary commitment of the receiving party to cooperate with the EEA SAs.
- 62. In the absence of a supervisory authority specifically in charge with the supervision of data protection law in the third country or at the international organisation, the need for an independent, effective and impartial supervisory oversight mechanism needs to be fulfilled by other means. The type of independent supervision mechanism put in place may depend on the case at hand.
- 63. The agreement could, for example, refer to existing oversight bodies in the third country other than a supervisory authority in the area of data protection. In addition, if no external independent oversight can be ensured from a structural or institutional point of view, e.g. because of the privileges and immunities of certain international organisations, oversight could be guaranteed through functionally autonomous mechanisms. The latter must be a body that, while not external itself, carries out its functions independently, i.e. free from instructions, with sufficient human, technical and financial resources, etc. The receiving party shall be bound by the decisions of the oversight body.

## 2.9 Termination clause

- 64. The international agreement should envisage that any personal data transferred from the EEA pursuant to the international agreement prior to its effective termination shall continue to be processed in accordance with the provisions of the international agreement.

---

<sup>29</sup> CJEU, October 6, 2015, Judgment in case C-362/14, Maximillian Schrems v Data Protection Commissioner (“Schrems”), paras 41 and 95.

<sup>30</sup> CJEU, July 27, 2017, Opinion 1/15 on the agreement envisaged between the European Union and Canada on the transfer of Passenger Name Record data, 26 July 2017, para. 228 and seq.; CJEU, 30 April 2019, Opinion 1/17 on the Comprehensive Economic and Trade agreement between Canada and the European Union, para. 190 and seq.

<sup>31</sup> ECtHR, September 6, 1978, Klass, v. Germany, para. 55 and 56. The requirement stemming from the ECtHR also apply to any interference with Articles 7 and 8 of the EU Charter since, according to Article 52 (3) EU Charter, the meaning and scope of these fundamental rights shall be the same as those laid down by Article 8 ECHR.

### 3 SPECIFIC INFORMATION ON ARTICLE 46 GDPR

#### 3.1 Specific information on legally binding and enforceable instruments - Article 46 (2) (a) GDPR

65. Article 46 (2) (a) GDPR allows EEA public bodies to base transfers to public bodies in a third country or an international organisation on instruments concluded between them without obtaining prior authorisation from a SA. Such instruments have to be legally binding and enforceable. Therefore, international treaties, public-law treaties or self-executing administrative agreements may be used under this provision.
66. Any legally binding and enforceable instrument should encompass the core set of data protection principles and data subject rights as required by the GDPR.
67. The parties are obliged to commit themselves to putting sufficient data protection safeguards for transferring data into place. As a consequence, the agreement should also set out the way in which the receiving public body will apply the core set of basic data protection principles and data subject rights to all transferred personal data in order to ensure that the level of protection of natural persons under the GDPR is not undermined.
68. If there is no possibility to ensure effective judicial redress in legally binding and enforceable instruments so that alternative redress mechanism have to be agreed upon, EEA public bodies should consult the competent SA before concluding these instruments.
69. Even if the form of the instrument is not decisive as long as it is legally binding and enforceable, the EDPB considers that the best option would be to incorporate detailed data protection clauses directly within the instrument. If, however, this solution is not feasible due to the particular circumstances, the EDPB strongly recommends incorporating at least a general clause setting out the data protection principles directly within the text of the instrument and inserting the more detailed provisions and safeguards in an annex to the instrument.

#### 3.2 Specific information on administrative arrangements - Article 46 (3) (b) GDPR

70. The GDPR in its Article 46 (3) (b) also provides for alternative instruments in the form of administrative arrangements, e.g. Memorandum of Understanding “MOU”, providing protection through the commitments taken by both parties in order to bring their common arrangement into force.
71. In this respect, Article 46 (1) and recital 108 of the GDPR specify that these arrangements have to ensure enforceable data subject rights and effective legal remedies. Where safeguards are provided for in administrative arrangements that are not legally binding, authorisation by the competent SA has to be obtained.
72. It should be carefully assessed whether or not to make use of non-legally binding administrative arrangements to provide safeguards in the public sector, in view of the purpose of the processing and the nature of the data at hand. If data protection rights and redress for EEA individuals are not provided for in the domestic law of the third country or the internal rules/regulatory framework of the international organisation, preference should be given to concluding a legally binding agreement. Irrespective of the type of instrument adopted, the measures in place have to be effective to ensure the appropriate implementation, enforcement and supervision.

73. In administrative arrangements specific steps have to be taken to ensure effective individual rights, redress and oversight. In particular, to ensure effective and enforceable rights, a non-binding instrument should contain assurances from the public body receiving the EEA personal data that individual rights are fully provided by its domestic law and can be exercised by EEA individuals under the same conditions as is the case for citizens and residents of the concerned third country. The same applies if administrative and judicial redress is available to EEA individuals in the domestic legal framework of the receiving public body. Similarly, international organisations should provide assurances about individual rights provided by their internal rules, as well as the available redress mechanisms.
74. If this is not the case, individual rights should be guaranteed by specific commitments from the parties, combined with procedural mechanisms to ensure their effectiveness and provide redress to the individual. These specific commitments and procedural mechanisms must make it possible, in practice, to ensure compliance with the level of protection essentially equivalent to that guaranteed within the EU by the GDPR.  
Such procedural mechanisms may, for example, include commitments of the parties to inform each other of requests from EEA individuals and to settle disputes or claims in a timely fashion.
75. In addition, in case such disputes or claims cannot be resolved in an amicable way between the parties themselves, independent and effective redress to the individual must be provided by alternative mechanisms, for example through a possibility for the individual to have recourse to an alternative dispute resolution mechanism, such as arbitration or mediation. Such alternative dispute resolution mechanism must be binding<sup>32</sup>.
76. Depending on the case at hand, a combination of all or some of the above measures should be provided for in the administrative agreement in order to ensure effective redress. Other measures not included in these guidelines could also be acceptable as long as they provide for independent and effective redress.
77. Each administrative arrangement developed in accordance with Article 46 (3) (b) GDPR will be examined by the competent SA on a case by case basis, followed by the relevant EDPB procedure, if applicable. The competent SA will base its examination on the general recommendations set out in these guidelines, but might also ask for more guarantees depending on the specific case.

---

<sup>32</sup> CJEU, July 16, 2020, Judgment in case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems ("Schrems II"), paras 189, 196 and seq.

## 4 PROCEDURAL QUESTIONS

78. Administrative arrangements established under Article 46 (3) (b) GDPR will be examined on a case-by-case basis due to the requirements for an authorisation by the competent SA which, according to Article 46 (4) GDPR shall apply the consistency mechanism pursuant to Article 64 (2) GDPR. When integrating alternative redress mechanisms in binding and enforceable instruments pursuant to Article 46 (2) (a) GDPR, the EDPB recommends also seeking advice from the competent SA. The EDPB strongly advises to consult the competent SA at an early stage.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

# Guidelines



**Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak**

**Adopted on 21 April 2020**

## Version history

Version 1.1	30 April 2020	Minor corrections
Version 1.0	21 April 2020	Adoption of the Guidelines

## Table of contents

1	Introduction.....	4
2	Application of the GDPR.....	4
3	Definitions .....	5
3.1	“Data concerning health” .....	5
3.2	“Processing for the purpose of scientific research” .....	5
3.3	“Further processing” .....	6
4	Legal basis for the processing.....	6
4.1	Consent .....	6
4.2	National legislations .....	7
5	Data protection principles .....	8
5.1	Transparency and information to data subjects .....	8
5.1.1	When must the data subject be informed? .....	8
5.1.2	Exemptions .....	8
5.2	Purpose limitation and presumption of compatibility .....	10
5.3	Data minimisation and storage limitation.....	10
5.4	Integrity and confidentiality.....	10
6	Exercise of the rights of data subjects .....	11
7	International data transfers for scientific research purposes.....	12
8	Summary.....	13

# The European Data Protection Board

Having regard to Article 70 (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"),

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,

## HAS ADOPTED THE FOLLOWING GUIDELINES

### 1 INTRODUCTION

1. Due to the COVID-19 pandemic, there are currently great scientific research efforts in the fight against the SARS-CoV-2 in order to produce research results as fast as possible.
2. At the same time, legal questions concerning the use of health data pursuant to Article 4 (15) GDPR for such research purposes keep arising. The present guidelines aim to shed light on the most urgent of these questions such as the legal basis, the implementation of adequate safeguards for such processing of health data and the exercise of the data subject rights.
3. Please note that the development of a further and more detailed guidance for the processing of health data for the purpose of scientific research is part of the annual work plan of the EDPB. Also, please note that the current guidelines do not revolve around the processing of personal data for epidemiological surveillance.

### 2 APPLICATION OF THE GDPR

4. Data protection rules (such as the GDPR) do not hinder measures taken in the fight against the COVID-19 pandemic.<sup>1</sup> The GDPR is a broad piece of legislation and provides for several provisions that allow to handle the processing of personal data for the purpose of scientific research connected to the COVID-19 pandemic in compliance with the fundamental rights to privacy and personal data protection.<sup>2</sup> The GDPR also foresees a specific derogation to the prohibition of processing of certain special categories of personal data, such as health data, where it is necessary for these purposes of scientific research.<sup>3</sup>
5. Fundamental Rights of the EU must be applied when processing health data for the purpose of scientific research connected to the COVID-19 pandemic. Neither the Data Protection Rules nor the Freedom of Science pursuant to Article 13 of the Charter of Fundamental Rights of the EU have

---

<sup>1</sup> See the Statement of the EDPB from 19.3.2020 on the general processing of personal data in the context of the COVID-19 outbreak, available at [https://edpb.europa.eu/our-work-tools/our-documents/other/statement-processing-personal-data-context-covid-19-outbreak\\_en](https://edpb.europa.eu/our-work-tools/our-documents/other/statement-processing-personal-data-context-covid-19-outbreak_en).

<sup>2</sup> See for example Article 5 (1) (b) and (e), Article 14(5) (b) and Article 17 (3) (d) GDPR.

<sup>3</sup> See for example Article 9 (2) (j) and Article 89 (2) GDPR.

precedence over the other. Rather, these rights and freedoms must be carefully assessed and balanced, resulting in an outcome which respects the essence of both.

### 3 DEFINITIONS

6. It is important to understand which processing operations benefit from the special regime foreseen in the GDPR and elaborated on in the present guidelines. Therefore, the terms “data concerning health”, “processing for the purpose of scientific research” as well as “further processing” (also referred to as “primary and secondary usage of health data”) must be defined.

#### 3.1 “Data concerning health”

7. According to Article 4 (15) GDPR, “data concerning health” means *“personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status”*. As indicated by Recital 53, data concerning health deserves higher protection, as the use of such sensitive data may have significant adverse impacts for data subjects. In the light of this and the relevant jurisprudence of the European Court of Justice (“ECJ”),<sup>4</sup> the term “data concerning health” must be given a wide interpretation.
8. Data concerning health can be derived from different sources, for example:
  1. Information collected by a health care provider in a patient record (such as medical history and results of examinations and treatments).
  2. Information that becomes health data by cross referencing with other data thus revealing the state of health or health risks (such as the assumption that a person has a higher risk of suffering heart attacks based on the high blood pressure measured over a certain period of time).
  3. Information from a “self check” survey, where data subjects answer questions related to their health (such as stating symptoms).
  4. Information that becomes health data because of its usage in a specific context (such as information regarding a recent trip to or presence in a region affected with COVID-19 processed by a medical professional to make a diagnosis).

#### 3.2 “Processing for the purpose of scientific research”

9. Article 4 GDPR does not entail an explicit definition of “processing for the purpose of scientific research”. As indicated by Recital 159, *“the term 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. In addition, it should take into account the Union’s objective under Article 179 (1) TFEU of achieving a European Research Area. Scientific research purposes should also include studies conducted in the public interest in the area of public health.”*
10. The former Article 29-Working-Party has already pointed out that the term may not be stretched beyond its common meaning though and understands that “scientific research” in this context means

---

<sup>4</sup> See for example, regarding the Directive 95/46/EC, ECJ 6.11.2003, C-101/01 (Lindqvist) paragraph 50.

*“a research project set up in accordance with relevant sector-related methodological and ethical standards, in conformity with good practice”.*<sup>5</sup>

### 3.3 “Further processing”

11. Finally, when talking about “processing of health data for the purpose of scientific research”, there are two types of data usages:
  1. Research on personal (health) data which consists in the use of data directly collected for the purpose of scientific studies (“primary use”).
  2. Research on personal (health) data which consists of the further processing of data initially collected for another purpose (“secondary use”).
12. **Example 1:** For conducting a clinical trial on individuals suspected to be infected with SARS-CoV-2, health data are collected and questionnaires are used. This is a case of “primary use” of health data as defined above.
13. **Example 2:** A data subject has consulted a health care provider as a patient regarding symptoms of the SARS-CoV-2. If health data recorded by the health care provider is being used for scientific research purposes later on, this usage is classified as further processing of health data (secondary use) that has been collected for another initial purpose.
14. The distinction between scientific research based on primary or secondary usage of health data will become particularly important when talking about the legal basis for the processing, the information obligations and the purpose limitation principle pursuant to Article 5 (1) (b) GDPR as outlined below.

## 4 LEGAL BASIS FOR THE PROCESSING

15. All processing of personal data concerning health must comply with the principles relating to processing set out in Article 5 GDPR and with one of the legal grounds and the specific derogations listed respectively in Article 6 and Article 9 GDPR for the lawful processing of this special category of personal data.<sup>6</sup>
16. Legal bases and applicable derogations for processing health data for the purpose of scientific research are provided for respectively in Article 6 and Article 9. In the following section, the rules concerning consent and respective national legislation are addressed. It has to be noted that there is no ranking between the legal bases stipulated in the GDPR.

### 4.1 Consent

17. The consent of the data subject, collected pursuant to Article 6 (1) (a) and Article 9 (2) (a) GDPR, may provide a legal basis for the processing of data concerning health in the COVID-19 context.
18. However, it has to be noted that all the conditions for explicit consent, particularly those found in Article 4 (11), Article 6 (1) (a), Article 7 and Article 9 (2) (a) GDPR, must be fulfilled. Notably, consent must be freely given, specific, informed, and unambiguous, and it must be made by way of a statement or “clear affirmative action”.

---

<sup>5</sup> See the Guidelines on Consent under Regulation 2016/679 of the former Article 29 Working-Party from 10.04.2018, WP259 rev.01, 17EN, page 27 (endorsed by the EDPB). Available at [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=623051](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051).

<sup>6</sup> See for example, regarding the Directive 95/46/EC ECJ 13.5.2014, C-131/12 (Google Spain), paragraph 71.

19. As stated in Recital 43, consent cannot be considered freely given if there is a clear imbalance between the data subject and the controller. It is therefore important that a data subject is not pressured and does not suffer from disadvantages if they decide not to give consent. The EDPB has already addressed consent in the context of clinical trials.<sup>7</sup> Further guidance, particularly on the topic of explicit consent, can be found in the consent guidelines of the former Article 29-Working-Party.<sup>8</sup>
20. **Example:** A survey is conducted as part of a non-interventional study on a given population, researching symptoms and the progress of a disease. For the processing of such health data, the researchers may seek the consent of the data subject under the conditions as stipulated in Article 7 GDPR.
21. In the view of the EDPB, the example above is *not* considered a case of “clear imbalance of power” as mentioned in Recital 43 and the data subject should be able to give the consent to the researchers.<sup>9</sup> In the example, the data subjects are not in a situation of whatsoever dependency with the researchers that could inappropriately influence the exercise of their free will and it is also clear that it will have no adverse consequences if they refuse to give their consent.
22. However, researchers should be aware that if consent is used as the lawful basis for processing, there must be a possibility for individuals to withdraw that consent at any time pursuant to Article 7 (3) GDPR. If consent is withdrawn, all data processing operations that were based on consent remain lawful in accordance with the GDPR, but the controller shall stop the processing actions concerned and if there is no other lawful basis justifying the retention for further processing, the data should be deleted by the controller.<sup>10</sup>

#### [4.2 National legislations](#)

23. Article 6 (1) e or 6 (1) f GDPR in combination with the enacted derogations under Article 9 (2) (j) or Article 9 (2) (i) GDPR can provide a legal basis for the processing of personal (health) data for scientific research. In the context of clinical trial this has already been clarified by the Board.<sup>11</sup>
24. **Example:** A large population based study conducted on medical charts of COVID-19 patients.
25. As outlined above, the EU as well as the national legislator of each Member State may enact specific laws pursuant to Article 9 (2) (j) or Article 9 (2) (i) GDPR to provide a legal basis for the processing of health data for the purpose of scientific research. Therefore, the conditions and the extent for such processing *vary* depending on the enacted laws of the particular Member State.
26. As stipulated in Article 9 (2) (i) GDPR, such laws shall provide “*for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy*”. As similarly stipulated in Article 9 (2) (j) GDPR, such enacted laws “*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*”.

---

<sup>7</sup> See Opinion 3/2019 of the EDPB from 23.1.2019 on concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR), available at [https://edpb.europa.eu/our-work-tools/our-documents/avis-art-70/opinion-32019-concerning-questions-and-answers-interplay\\_en](https://edpb.europa.eu/our-work-tools/our-documents/avis-art-70/opinion-32019-concerning-questions-and-answers-interplay_en).

<sup>8</sup> Guidelines on Consent under Regulation 2016/679 of the former Article 29 Working-Party from 10.04.2018, WP259 rev.01, 17EN, page 18 (endorsed by the EDPB).

<sup>9</sup> Assuming that the data subject has not been pressured or threatened with disadvantages when not giving his or her consent.

<sup>10</sup> See Article 17 (1) (b) and (3) GDPR.

<sup>11</sup> See Opinion 3/2019 of the EDPB from 23.1.2019, page 7.

27. Furthermore, such enacted laws must be interpreted in the light of the principles pursuant to Article 5 GDPR and in consideration of the jurisprudence of the ECJ. In particular, derogations and limitations in relation to the protection of data provided in Article 9 (2) (j) and Article 89 GDPR must apply only in so far as is strictly necessary.<sup>12</sup>

## 5 DATA PROTECTION PRINCIPLES

28. The principles relating to processing of personal data pursuant to Article 5 GDPR shall be respected by the controller and processor, especially considering that a great amount of personal data may be processed for the purpose of scientific research. Considering the context of the present guidelines, the most important aspects of these principles are addressed in the following.

### 5.1 Transparency and information to data subjects

29. The principle of transparency means that personal data shall be processed fairly and in a transparent manner in relation to the data subject. This principle is strongly connected with the information obligations pursuant to Article 13 or Article 14 GDPR.
30. In general, a data subject must be individually informed of the existence of the processing operation and that personal (health) data is being processed for scientific purposes. The information delivered should contain all the elements stated in Article 13 or Article 14 GDPR.
31. It has to be noted that researchers often process health data that they have not obtained directly from the data subject, for instance using data from patient records or data from patients in other countries. Therefore, Article 14 GDPR, which covers information obligations where personal data is not collected directly from the data subject, will be the focus of this section.

#### 5.1.1 When must the data subject be informed?

32. When personal data have not been obtained from the data subject, Article 14 (3) (a) GDPR stipulates that the controller shall provide the information “*within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed*”.
33. In the current context, it has to be particularly noted that according to Article 14 (4) GDPR, where “*the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose*”.
34. In the case of the further processing of data for scientific purposes and taking into account the sensitivity of the data processed, an appropriate safeguard according to Article 89 (1) is to deliver the information to the data subject within a reasonable period of time *before* the implementation of the new research project. This allows the data subject to become aware of the research project and enables the possibility to exercise his/her rights beforehand.

#### 5.1.2 Exemptions

35. However, Article (14) (5) GDPR stipulates four exemptions of the information obligation. In the current context, the exemption pursuant to Article (14) (5) (b) (“proves impossible or would involve a disproportionate effort”) and (c) (“obtaining or disclosure is expressly laid down by Union or Member

---

<sup>12</sup> See for example, regarding the Directive 95/46/EC ECJ 14.2.2019, C-345/17 (Buivids) paragraph 64.

State law“) GDPR are of particular relevance, especially for the information obligation pursuant to Article 14 (4) GDPR.

#### 5.1.2.1 *Proves impossible*

36. In its Guidelines regarding the principle of Transparency,<sup>13</sup> the former Article 29-Working-Party has already pointed out that “*the situation where it “proves impossible” under Article 14 (5) (b) to provide the information is an all or nothing situation because something is either impossible or it is not; there are no degrees of impossibility. Thus, if a data controller seeks to rely on this exemption it must demonstrate the factors that actually prevent it from providing the information in question to data subjects. If, after a certain period of time, the factors that caused the “impossibility” no longer exist and it becomes possible to provide the information to data subjects then the data controller should immediately do so. In practice, there will be very few situations in which a data controller can demonstrate that it is actually impossible to provide the information to data subjects.*”

#### 5.1.2.2 *Disproportionate effort*

37. In determining what constitutes disproportionate effort, Recital 62 refers to the number of data subjects, the age of the data and appropriate safeguards in place as possible indicative factors. In the Transparency Guidelines mentioned above,<sup>14</sup> it is recommended that the controller should therefore carry out a balancing exercise to assess the effort involved to provide the information to data subjects against the impact and effects on the data subject if they are not provided with the information.
38. **Example:** A large number of data subjects where there is no available contact information could be considered as a disproportionate effort to provide the information.

#### 5.1.2.3 *Serious impairment of objectives*

39. To rely on this exception, data controllers must demonstrate that the provision of the information set out in Article 14 (1) *per se* would render impossible or seriously impair the achievement of the objectives of the processing.
40. In a case where the exemption of Article (14) (5) (b) GDPR applies, “*the controller shall take appropriate measures to protect the data subject’s rights and freedoms and legitimate interests, including making the information publicly available*”.

#### 5.1.2.4 *Obtaining or disclosure is expressly laid down by Union or Member State law*

41. Article 14 (5) (c) GDPR allows for a derogation of the information requirements in Articles 14 (1), (2) and (4) insofar as the obtaining or disclosure of personal data “*is expressly laid down by Union or Member State law to which the controller is subject*”. This exemption is conditional upon the law in question providing “*appropriate measures to protect the data subject’s legitimate interests*”. As stated in the above mentioned Transparency Guidelines,<sup>15</sup> such law must directly address the data controller and the obtaining or disclosure in question should be mandatory upon the data controller. When relying on this exemption, the EDPB recalls that the data controller must be able to demonstrate how

---

<sup>13</sup> See the Guidelines on transparency under Regulation 2016/679 of the former Article-29 Working-Party from 11.4.2018, WP260 rev.01, 17/EN, page 29 (endorsed by the EDPB). Available at [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=622227](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227).

<sup>14</sup> Guidelines on transparency under Regulation 2016/679 of the former Article-29 Working-Party from 11.4.2018, WP260 rev.01, 17/EN, page 31 (endorsed by the EDPB).

<sup>15</sup> Guidelines on transparency under Regulation 2016/679 of the former Article-29 Working-Party from 11.4.2018, WP260 rev.01, 17/EN, page 32 (endorsed by the EDPB).

the law in question applies to them and requires them to either obtain or disclose the personal data in question.

### 5.2 Purpose limitation and presumption of compatibility

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).<sup>16</sup> 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.

### 5.3 Data minimisation and storage limitation

46. In scientific research, data minimisation can be achieved through the requirement of specifying the research questions and assessing the type and amount of data necessary to properly answer these research questions. Which data is needed depends on the purpose of the research even when the research has an explorative nature and should always comply with the purpose limitation principle pursuant to Article 5 (1) (b) GDPR. It has to be noted that the data has to be anonymised where it is possible to perform the scientific research with anonymised data.
47. In addition, proportionate storage periods shall be set. As stipulated by Article 5 (1) (e) GDPR “*personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving [...] scientific purposes [...] in accordance with Article 89 (1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject*”
48. In order to define storage periods (timelines), criteria such as the length and the purpose of the research should be taken into account. It has to be noted that national provisions may stipulate rules concerning the storage period as well.

### 5.4 Integrity and confidentiality

49. As mentioned above, sensitive data such as health data merit higher protection as their processing is likelier to lead to negative impacts for data subjects. This consideration especially applies in the COVID-

---

<sup>16</sup> Also see the Guidelines 4/2019 of the EDPB from 13.11.2019 on Data Protection by Design and by Default (version for public consultation), available at [https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design\\_en](https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en)

- 19 outbreak as the foreseeable re-use of health data for scientific purposes leads to an increase in the number and type of entities processing such data.
- 50. It has to be noted that the principle of integrity and confidentiality must be read in conjunction with the requirements of Article 32 (1) GDPR and Article 89 (1) GDPR. The cited provisions must be fully complied with. Therefore, considering the high risks as outlined above, appropriate technical and organisational up-to-date measures must be implemented to ensure a sufficient level of security.
  - 51. Such measures should *at least* consist of pseudonymisation,<sup>17</sup> encryption, non-disclosure agreements and strict access role distribution, access role restrictions as well as access logs. It has to be noted that national provisions may stipulate concrete technical requirements or other safeguards such as adherence to professional secrecy rules.
  - 52. Furthermore, a data protection impact assessment pursuant to Article 35 GDPR must be carried out when such processing is "*likely to result in a high risk to the rights and freedoms of natural persons*" pursuant to Article 35 (1) GDPR. The lists pursuant to Article 35 (4) and (5) GDPR shall be taken into account.
  - 53. At this point, the EDPB emphasises the importance of data protection officers. Where applicable, data protection officers should be consulted on processing of health data for the purpose of scientific research in the context of the COVID-19 outbreak.
  - 54. Finally, the adopted measures to protect data (including during transfers) should be properly documented in the record of processing activities.

## 6 EXERCISE OF THE RIGHTS OF DATA SUBJECTS

- 55. In principle, situations as the current COVID-19 outbreak do not suspend or restrict the possibility of data subjects to exercise their rights pursuant to Article 12 to 22 GDPR. However, Article 89 (2) GDPR allows the national legislator to restrict (some) of the data subject's rights as set in Chapter 3 of the regulation. Because of this, the restrictions of the rights of data subjects *may vary* depending on the enacted laws of the particular Member State.
- 56. Furthermore, some restrictions of the rights of data subjects can be based directly on the Regulation, such as the access right restriction pursuant to Article 15 (4) GDPR and the restriction of the right to erasure pursuant to Article 17 (3) (d) GDPR. The information obligation exemptions pursuant to Article 14 (5) GDPR have already been addressed above.
- 57. It has to be noted that, in the light of the jurisprudence of the ECJ, all restrictions of the rights of data subjects must apply only in so far as it is strictly necessary.<sup>18</sup>

---

<sup>17</sup> It has to be noted that personal (health data) that has been pseudonymised is still regarded as "personal data" pursuant to Article 4 (1) GDPR and must not be confused with "anonymised data" where it is no longer possible for anyone to refer back to individual data subjects. See for example Recital 28.

<sup>18</sup> See for example, regarding the Directive 95/46/EC ECJ 14.2.2019, C-345/17 (Buivids) paragraph 64.

## 7 INTERNATIONAL DATA TRANSFERS FOR SCIENTIFIC RESEARCH PURPOSES

58. Within the context of research and specifically in the context of the COVID-19 pandemic, there will probably be a need for international cooperation that may also imply international transfers of health data for the purpose of scientific research outside of the EEA.
59. When personal data is transferred to a non-EEA country or international organisation, in addition to complying with the rules set out in GDPR,<sup>19</sup> especially its Articles 5 (data protection principles), Article 6 (lawfulness) and Article 9 (special categories of data),<sup>20</sup> the data exporter shall also comply with Chapter V (data transfers).<sup>21</sup>
60. In addition to the regular transparency requirement as mentioned on page 7 of the present guidelines, a duty rests on the data exporter to inform data subjects that it intends to transfer personal data to a third country or international organisation. This includes information about the existence or absence of an adequacy decision by the European Commission, or whether the transfer is based on a suitable safeguard from Article 46 or on a derogation of Article 49 (1). This duty exists irrespective of whether the personal data was obtained directly from the data subject or not.
61. In general, when considering how to address such conditions for transfers of personal data to third countries or international organisations, data exporters should assess the risks to the rights and the freedoms of data subjects of each transfer<sup>22</sup> and favour solutions that guarantee data subjects the continuous protection of their fundamental rights and safeguards as regards the processing of their data, even after it has been transferred. This will be the case for transfers to countries having an adequate level of protection,<sup>23</sup> or in case of use of one of the appropriate safeguards included in Article 46 GDPR,<sup>24</sup> ensuring that enforceable rights and effective legal remedies are available for data subjects.
62. In the absence of an adequacy decision pursuant to Article 45 (3) GDPR or appropriate safeguards pursuant to Article 46 GDPR, Article 49 GDPR envisages certain specific situations under which transfers of personal data can take place as an exception. The derogations enshrined in Article 49 GDPR are thus exemptions from the general rule and, therefore, must be interpreted restrictively, and on a case-by-case basis.<sup>25</sup> Applied to the current COVID-19 crisis, those addressed in Article 49 (1) (d) ("transfer necessary for important reasons of public interest") and (a) ("explicit consent") may apply.
63. The COVID-19 pandemic causes an exceptional sanitary crisis of an unprecedented nature and scale. In this context, the EDPB considers that the fight against COVID-19 has been recognised by the EU and

---

<sup>19</sup> Article 44 GDPR.

<sup>20</sup> See sections 4 to 6 of the present Guidelines.

<sup>21</sup> See the Guidelines 2/2018 of the EDPB from 25.5.2018 on derogations of Article 49 under Regulation 2016/679, page 3, on the two-step test, available at [https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-2018-derogations-article-49-under-regulation\\_en](https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-2018-derogations-article-49-under-regulation_en).

<sup>22</sup> International Data Transfers maybe a risk factor to consider when performing a DPIA as referred to in page 10 of the present guidelines.

<sup>23</sup> The list of countries recognised adequate by the European Commission is available at [https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en)

<sup>24</sup> For example standard data protection clauses pursuant to Article 46 (2) (c) or (d) GDPR, ad hoc contractual clauses pursuant to Article 46 (3) (a) GDPR or administrative arrangements pursuant to Article 46 (3) (b) GDPR.

<sup>25</sup> See Guidelines 2/2018, page 3.

most of its Member States as an important public interest,<sup>26</sup> which may require urgent action in the field of scientific research (for example to identify treatments and/or develop vaccines), and may also involve transfers to third countries or international organisations.<sup>27</sup>

64. Not only public authorities, but also private entities playing a role in pursuing such public interest (for example, a university's research institute cooperating on the development of a vaccine in the context of an international partnership) could, under the current pandemic context, rely upon the derogation mentioned above.
65. In addition, in certain situations, in particular where transfers are performed by private entities for the purpose of medical research aiming at fighting the COVID-19 pandemic,<sup>28</sup> such transfers of personal data could alternatively take place on the basis of the explicit consent of the data subjects.<sup>29</sup>
66. Public authorities and private entities may, under the current pandemic context, when it is not possible to rely on an adequacy decision pursuant to Article 45 (3) or on appropriate safeguards pursuant to Article 46, rely upon the applicable derogations mentioned above, mainly as a temporary measure due to the urgency of the medical situation globally.
67. Indeed, if the nature of the COVID-19 crisis may justify the use of the applicable derogations for initial transfers carried out for the purpose of research in this context, repetitive transfers of data to third countries part of a long lasting research project in this regard would need to be framed with appropriate safeguards in accordance with Article 46 GDPR.<sup>30</sup>
68. Finally, it has to be noted that any such transfers will need to take into consideration on a case-by-case basis the respective roles (controller, processor, joint controller) and related obligations of the actors involved (sponsor, investigator) in order to identify the appropriate measures for framing the transfer.

## 8 SUMMARY

69. The key findings of these guidelines are:

1. The GDPR provides special rules for the processing of health data for the purpose of scientific research that are also applicable in the context of the COVID-19 pandemic.
2. The national legislator of each Member State may enact specific laws pursuant to Article (9) (2) (i) and (j) GDPR to enable the processing of health data for scientific research purposes. The processing of health data for the purpose of scientific research must also be covered by

---

<sup>26</sup> Article 168 of the Treaty on the Functioning of the European Union recognises a high level of human health protection as an important objective that should be ensured in the implementation of all Union policies and activities. On this basis, Union action supports national policies to improve public health, including in combatting against major health scourges and serious cross-border threats to health, e.g. by promoting research into their causes, transmission and prevention. Similarly, Recitals 46 and 112 of the GDPR refer to processing carried out in the context of the fight against epidemics as an example of processing serving important grounds of public interest. In the context of the COVID-19 pandemic, the EU has adopted a series of measures in a broad range of areas (e.g. funding of healthcare systems, support to cross-border patients and deployment of medical staff, financial assistance to the most deprived, transport, medical devices etc.) premised on the understanding that the EU is facing a major public health emergency requiring an urgent response.

<sup>27</sup> The EDPB underlines that the GDPR, in its Recital 112, refers to the international data exchange between services competent for public health purposes as an example of the application of this derogation.

<sup>28</sup> In accordance with Article 49 (3) GDPR, consent cannot be used for activities carried out by public authorities in the exercise of their public powers.

<sup>29</sup> See EDPB Guidelines 2/2018, section 2.1.

<sup>30</sup> See EDPB Guidelines 2/2018, page 5.

one of the legal bases in Article 6 (1) GDPR. Therefore, the conditions and the extent for such processing varies depending on the enacted laws of the particular member state.

3. All enacted laws based on Article (9) (2) (i) and (j) GDPR must be interpreted in the light of the principles pursuant to Article 5 GDPR and in consideration of the jurisprudence of the ECJ. In particular, derogations and limitations in relation to the protection of data provided in Article 9 (2) (j) and Article 89 (2) GDPR must apply only in so far as is strictly necessary.
4. Considering the processing risks in the context of the COVID-19 outbreak, high emphasise must be put on compliance with Article 5 (1) (f), Article 32 (1) and Article 89 (1) GDPR. There must be an assessment if a DPIA pursuant to Article 35 GDPR has to be carried out.
5. Storage periods (timelines) shall be set and must be proportionate. In order to define such storage periods, criteria such as the length and the purpose of the research should be taken into account. National provisions may stipulate rules concerning the storage period as well and must therefore be considered.
6. In principle, situations as the current COVID-19 outbreak do not suspend or restrict the possibility of data subjects to exercise their rights pursuant to Article 12 to 22 GDPR. However, Article 89 (2) GDPR allows the national legislator to restrict (some) of the data subject's rights as set in Chapter 3 of the GDPR. Because of this, the restrictions of the rights of data subjects *may vary* depending on the enacted laws of the particular Member State.
7. With respect to international transfers, in the absence of an adequacy decision pursuant to Article 45 (3) GDPR or appropriate safeguards pursuant to Article 46 GDPR, public authorities and private entities may rely upon the applicable derogations pursuant to Article 49 GDPR. However, the derogations of Article 49 GDPR do have exceptional character only.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

# Guidelines



**Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak**

**Adopted on 21 April 2020**

## Table of contents

Table of contents.....	2
1    Introduction & context.....	3
2    Use of location data .....	5
2.1    Sources of location data .....	5
2.2    Focus on the use of anonymised location data.....	5
3    contact tracing applications .....	7
3.1    General legal analysis .....	7
3.2    Recommendations and functional requirements .....	9
4    Conclusion .....	10
Annex -- Contact Tracing Applications Analysis Guide.....	11

# The European Data Protection Board

Having regard to Article 70(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"),

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<sup>1</sup>,

Having regard to Article 12 and Article 22 of its Rules of Procedure,

## **HAS ADOPTED THE FOLLOWING GUIDELINES:**

### **1 INTRODUCTION & CONTEXT**

- 1 Governments and private actors are turning toward the use of data driven solutions as part of the response to the COVID-19 pandemic, raising numerous privacy concerns.
- 2 The EDPB underlines that the data protection legal framework was designed to be flexible and as such, is able to achieve both an efficient response in limiting the pandemic and protecting fundamental human rights and freedoms.
- 3 The EDPB firmly believes that, when processing of personal data is necessary for managing the COVID-19 pandemic, data protection is indispensable to build trust, create the conditions for social acceptability of any solution, and thereby guarantee the effectiveness of these measures. Because the virus knows no borders, it seems preferable to develop a common European approach in response to the current crisis, or at least put in place an interoperable framework.
- 4 The EDPB generally considers that data and technology used to help fight COVID-19 should be used to empower, rather than to control, stigmatise, or repress individuals. Furthermore, while data and technology can be important tools, they have intrinsic limitations and can merely leverage the effectiveness of other public health measures. 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-19.
- 5 These guidelines clarify the conditions and principles for the proportionate use of location data and contact tracing tools, for two specific purposes:
  - ) using location data to support the response to the pandemic by modelling the spread of the virus so as to assess the overall effectiveness of confinement measures ;
  - ) contact tracing, which aims to notify individuals of the fact that they have been in close proximity of someone who is eventually confirmed to be a carrier of the virus, in order to break the contamination chains as early as possible.
- 6 The efficiency of the contribution of contact tracing applications to the management of the pandemic depends on many factors (e.g., percentage of people who would need to install it; definition of a "contact" in terms of closeness and duration.). Moreover, such applications need to be part of a comprehensive public health strategy to fight the pandemic, including, inter alia, testing and subsequent manual contact tracing for the purpose of doubt removal. Their

---

<sup>1</sup> References to "Member States" made throughout this document should be understood as references to "EEA Member States".

deployment should be accompanied by supporting measures to ensure that the information provided to the users is contextualized, and that alerts can be of use to the public health system. Otherwise, these applications might not reach their full impact.

- 7 The EDPB emphasises that the GDPR and Directive 2002/58/EC (the “ePrivacy Directive”) both contain specific rules allowing for the use of anonymous or personal data to support public authorities and other actors at national and EU levels in monitoring and containing the spread of the SARS-CoV-2 virus<sup>2</sup>.
- 8 In this regard, the EDPB has already taken position on the fact that the use of contact tracing applications should be voluntary and should not rely on tracing individual movements but rather on proximity information regarding users.<sup>3</sup>

---

<sup>2</sup> See the [previous statement of the EDPB on the COVID 19 outbreak](#).

<sup>3</sup> [https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletttereccodiv-appguidance\\_final.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletttereccodiv-appguidance_final.pdf)

## 2 USE OF LOCATION DATA

### 2.1 Sources of location data

- 9 There are two principal sources of location data available for modelling the spread of the virus and the overall effectiveness of confinement measures:
- \_) location data collected by electronic communication service providers (such as mobile telecommunication operators) in the course of the provision of their service ; and
  - \_) location data collected by information society service providers' applications whose functionality requires the use of such data (e.g., navigation, transportation services, etc.).
- 10 The EDPB recalls that location data<sup>4</sup> collected from electronic communication providers may only be processed within the remits of articles 6 and 9 of the ePrivacy Directive. This means that these data can only be transmitted to authorities or other third parties if they have been anonymised by the provider or, for data indicating the geographic position of the terminal equipment of a user, which are not traffic data, with the prior consent of the users<sup>5</sup>.
- 11 Regarding information, including location data, collected directly from the terminal equipment, art. 5(3) of the “ePrivacy” directive applies. Hence, the storing of information on the user’s device or gaining access to the information already stored is allowed only if (i) the user has given consent<sup>6</sup> or (ii) the storage and/or access is strictly necessary for the information society service explicitly requested by the user.
- 12 Derogations to the rights and obligations provided for in the “ePrivacy” Directive are however possible pursuant to Art. 15, when they constitute a necessary, appropriate and proportionate measure within a democratic society for certain objectives<sup>7</sup>.
- 13 As for the re-use of location data collected by an information society service provider for modelling purposes (e.g., through the operating system or some previously installed application) additional conditions must be met. Indeed, when data have been collected in compliance with Art. 5(3) of the ePrivacy Directive, they can only be further processed with the additional consent of the data subject or on the basis of a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Art. 23 (1) GDPR.<sup>8</sup>

### 2.2 Focus on the use of anonymised location data

- 14 The EDPB emphasises that when it comes to using location data, preference should always be given to the processing of anonymised data rather than personal data.
- 15 Anonymisation refers to the use of a set of techniques in order to remove the ability to link the data with an identified or identifiable natural person against any “reasonable” effort. This “reasonability test” must take into account both objective aspects (time, technical means) and contextual elements that may vary case by case (rarity of a phenomenon including population density, nature and volume of data). If the data fails to pass this test, then it has not been anonymised and therefore remains in the scope of the GDPR.
- 16 Evaluating the robustness of anonymisation relies on three criteria: (i) singling-out (isolating an individual in a larger group based on the data); (ii) linkability (linking together two records

---

<sup>4</sup>See Art. 2(c) of the ePrivacy Directive.

<sup>5</sup> See Art 6 and 9 of the ePrivacy Directive.

<sup>6</sup> The notion of consent in the ePrivacy directive remains the notion of consent in the GDPR and must meet all the requirements of the consent as provided by art. 4(11) and 7 GDPR

<sup>7</sup> For the interpretation of article 15 of the “ePrivacy” Directive, see also, CJEU Judgment of 29 January 2008 in case C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU.

<sup>8</sup> See section 1.5.3 of the guidelines 1/2020 on processing personal data in the context of connected vehicles.

- concerning the same individual); and (iii) inference (deducing, with significant probability, unknown information about an individual).
- 17 The concept of anonymisation is prone to being misunderstood and is often mistaken for pseudonymisation. While anonymisation allows using the data without any restriction, pseudonymised data are still in the scope of the GDPR.
  - 18 Many options for effective anonymisation exist<sup>9</sup>, but with a caveat. Data cannot be anonymised on their own, meaning that only datasets as a whole may or may not be made anonymous. In this sense, any intervention on a single data pattern (by means of encryption, or any other mathematical transformations) can at best be considered a pseudonymisation.
  - 19 Anonymisation processes and re-identification attacks are active fields of research. It is crucial for any controller implementing anonymisation solutions to monitor recent developments in this field, especially concerning location data (originating from telecom operators and/or information society services) which are known to be notoriously difficult to anonymise.
  - 20 Indeed, a large body of research has shown<sup>10</sup> that *location data thought to be anonymised* may in fact not be. Mobility traces of individuals are inherently highly correlated and unique. Therefore, they can be vulnerable to re-identification attempts under certain circumstances.
  - 21 A single data pattern tracing the location of an individual over a significant period of time cannot be fully anonymised. This assessment may still hold true if the precision of the recorded geographical coordinates is not sufficiently lowered, or if details of the track are removed and even if only the location of places where the data subject stays for substantial amounts of time are retained. This also holds for location data that is poorly aggregated.
  - 22 To achieve anonymisation, location data must be carefully processed in order to meet the reasonability test. In this sense, such a processing includes considering location datasets as a whole, as well as processing data from a reasonably large set of individuals using available robust anonymisation techniques, provided that they are adequately and effectively implemented.
  - 23 Lastly, given the complexity of anonymisation processes, transparency regarding the anonymisation methodology is highly encouraged.

---

<sup>9</sup> (de Montjoye et al., 2018) "[On the privacy-conscious use of mobile phone data](#)"

<sup>10</sup> (de Montjoye et al., 2013) "[Unique in the Crowd: The privacy bounds of human mobility](#)" and (Pyrgelis et al., 2017) "[Knock Knock, Who's There? Membership Inference on Aggregate Location Data](#)"

### 3 CONTACT TRACING APPLICATIONS

#### 3.1 General legal analysis

- 24 The systematic and large scale monitoring of location and/or contacts between natural persons is a grave intrusion into their privacy. It can only be legitimised by relying on a voluntary adoption by the users for each of the respective purposes. This would imply, in particular, that individuals who decide not to or cannot use such applications should not suffer from any disadvantage at all.
- 25 To ensure accountability, the controller of any contact tracing application should be clearly defined. The EDPB considers that the national health authorities could be the controllers<sup>11</sup> for such application; other controllers may also be envisaged. In any cases, if the deployment of contact tracing apps involves different actors their roles and responsibilities must be clearly established from the outset and be explained to the users.
- 26 In addition, with regard to the principle of purpose limitation, the purposes must be specific enough to exclude further processing for purposes unrelated to the management of the COVID-19 health crisis (e.g., commercial or law enforcement purposes). Once the objective has been clearly defined, it will be necessary to ensure that the use of personal data is adequate, necessary and proportionate.
- 27 In the context of a contact tracing application, careful consideration should be given to the principle of data minimisation and data protection by design and by default:
- ✓ contact tracing apps do not require tracking the location of individual users. Instead, proximity data should be used;
  - ✓ as contact tracing applications can function without direct identification of individuals, appropriate measures should be put in place to prevent re-identification;
  - ✓ the collected information should reside on the terminal equipment of the user and only the relevant information should be collected when absolutely necessary.
- 28 Regarding the lawfulness of the processing, the EDPB notes that contact tracing applications involve storage and/or access to information already stored in the terminal, which are subject to Art. 5(3) of the “ePrivacy” Directive. If those operations are strictly necessary in order for the provider of the application to provide the service explicitly requested by the user the processing would not require his/her consent. For operations that are not strictly necessary, the provider would need to seek the consent of the user.
- 29 Furthermore, the EDPB notes that the mere fact that the use of contact-tracing applications takes place on a voluntary basis does not mean that the processing of personal data will necessarily be based on consent. When public authorities provide a service based on a mandate assigned by and in line with requirements laid down by law, it appears that the most relevant legal basis for the processing is the necessity for the performance of a task in the public interest, i.e. Art. 6(1)(e) GDPR.
- 30 Article 6(3) GDPR clarifies that the basis for the processing referred to in article 6(1)(e) shall be laid down by Union or Members 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.<sup>12</sup>
- 31 The legal basis or legislative measure that provides the lawful basis for the use of contact tracing applications should, however, incorporate meaningful safeguards including a reference to the voluntary nature of the application. A clear specification of purpose and explicit

---

<sup>11</sup> See also European Commission “Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection” Brussels, 16.4.2020 C(2020) 2523 final.

<sup>12</sup> See Recital (41).

limitations concerning the further use of personal data should be included, as well as a clear identification of the controller(s) involved. The categories of data as well as the entities to (and purposes for which, the personal data may be disclosed) should also be identified. Depending on the level of interference, additional safeguards should be incorporated, taking into account the nature, scope and purposes of the processing. Finally, the EDPB also recommends including, as soon as practicable, the criteria to determine when the application shall be dismantled and which entity shall be responsible and accountable for making that determination.

- 32 However, if the data processing is based on another legal basis, such as consent (Art. 6(1)(a))<sup>13</sup> for example, the controller will have to ensure that the strict requirements for such legal basis to be valid are met.
- 33 Moreover, the use of an application to fight the COVID-19 pandemic might lead to the collection of health data (for example the status of an infected person). Processing of such data is allowed when such processing is necessary for reasons of public interest in the area of public health, meeting the conditions of art. 9(2)(i) GDPR<sup>14</sup> or for health care purposes as described in Art. 9(2)(h) GDPR<sup>15</sup>. Depending on the legal basis, it might also be based on explicit consent (Art. 9(2)(a) GDPR).
- 34 In accordance with the initial purpose, Article 9(2)(j) GDPR also allows for health data to be processed when necessary for scientific research purposes or statistical purposes.
- 35 The current health crisis should not be used as an opportunity to establish disproportionate data retention mandates. Storage limitation should consider the true needs and the medical relevance (this may include epidemiology-motivated considerations like the incubation period, etc.) and personal data should be kept only for the duration of the COVID-19 crisis. Afterwards, as a general rule, all personal data should be erased or anonymised.
- 36 It is the EDPB's understanding that such apps cannot replace, but only support, manual contact tracing performed by qualified public health personnel, who can sort out whether close contacts are likely to result in virus transmission or not (e.g., when interacting with someone protected by adequate equipment – cashiers, etc. -- or not). The EDPB underlines that procedures and processes including respective algorithms implemented by the contact tracing apps should work under the strict supervision of qualified personnel in order to limit the occurrence of any false positives and negatives. In particular, the task of providing advice on next steps should not be based solely on automated processing.
- 37 In order to ensure their fairness, accountability and, more broadly, their compliance with the law, algorithms must be auditable and should be regularly reviewed by independent experts. The application's source code should be made publicly available for the widest possible scrutiny.
- 38 False positives will always occur to a certain degree. As the identification of an infection risk probably can have a high impact on individuals, such as remaining in self isolation until tested negative, the ability to correct data and/or subsequent analysis results is a necessity. This, of course, should only apply to scenarios and implementations where data is processed and/or stored in a way where such correction is technically feasible and where the adverse effects mentioned above are likely to happen.
- 39 Finally the EDPB considers that a data protection impact assessment (DPIA) must be carried out before implementing such tool as the processing is considered likely high risk (health data,

---

<sup>13</sup> Controllers (especially public authorities) must pay special attention to the fact that consent should not be regarded as freely given if the individual has no genuine choice to refuse or withdraw its consent without detriment.

<sup>14</sup> The processing must be based on Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

<sup>15</sup> See Article 9(2)(h) GDPR

anticipated large-scale adoption, systematic monitoring, use of new technological solution)<sup>16</sup>. The EDPB strongly recommends the publication of DPIAs.

### 3.2 Recommendations and functional requirements

- 40 According to the principle of data minimization, among other measures of Data Protection by Design and by Default<sup>17</sup>, the data processed should be reduced to the strict minimum. The application should not collect unrelated or not needed information, which may include civil status, communication identifiers, equipment directory items, messages, call logs, location data, device identifiers, etc.
- 41 Data broadcasted by applications must only include some unique and pseudonymous identifiers, generated by and specific to the application. Those identifiers must be renewed regularly, at a frequency compatible with the purpose of containing the spread of the virus, and sufficient to limit the risk of identification and of physical tracking of individuals.
- 42 Implementations for contact tracing can follow a centralized or a decentralized approach<sup>18</sup>. Both should be considered viable options, provided that adequate security measures are in place, each being accompanied by a set of advantages and disadvantages. Thus, the conceptual phase of app development should always include thorough consideration of both concepts carefully weighing up the respective effects on data protection /privacy and the possible impacts on individuals rights.
- 43 Any server involved in the contact tracing system must only collect the contact history or the pseudonymous identifiers of a user diagnosed as infected as the result of a proper assessment made by health authorities and of a voluntary action of the user. Alternately, the server must keep a list of pseudonymous identifiers of infected users or their contact history only for the time to inform potentially infected users of their exposure, and should not try to identify potentially infected users.
- 44 Putting in place a global contact tracing methodology including both applications and manual tracing may require additional information to be processed in some cases. In this context, this additional information should remain on the user terminal and only be processed when strictly necessary and with his prior and specific consent.
- 45 State-of-the-art cryptographic techniques must be implemented to secure the data stored in servers and applications, exchanges between applications and the remote server. Mutual authentication between the application and the server must also be performed.
- 46 The reporting of users as COVID-19 infected on the application must be subject to proper authorization, for example through a single-use code tied to a pseudonymous identity of the infected person and linked to a test station or health care professional. If confirmation cannot be obtained in a secure manner, no data processing should take place that presumes the validity of the user's status.
- 47 The controller, in collaboration with the public authorities, have to clearly and explicitly inform about the link to download the official national contact tracing app in order to mitigate the risk that individuals use a third-party app.

---

<sup>16</sup> See WP29 guidelines (adopted by the EDPB) on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679.

<sup>17</sup> See EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default

<sup>18</sup> In general, the decentralised solution is more in line with the minimisation principle

## 4 CONCLUSION

- 48 The world is facing a significant public health crisis that requires strong responses, which will have an impact beyond this emergency. Automated data processing and digital technologies can be key components in the fight against COVID-19. However, one should be wary of the “ratchet effect”. It is our responsibility to ensure that every measure taken in these extraordinary circumstances are necessary, limited in time, of minimal extent and subject to periodic and genuine review as well as to scientific evaluation.
- 49 The EDPB underlines that one should not have to choose between an efficient response to the current crisis and the protection of our fundamental rights: we can achieve both, and moreover data protection principles can play a very important role in the fight against the virus. European data protection law allows for the responsible use of personal data for health management purposes, while also ensuring that individual rights and freedoms are not eroded in the process.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

# ANNEX -- CONTACT TRACING APPLICATIONS

## ANALYSIS GUIDE

### 0. Disclaimer

The following guidance is neither prescriptive nor exhaustive, and its sole purpose of this guide is to provide general guidance to designers and implementers of contact tracing applications. Other solutions than the ones described here can be used and can be lawful as long as they comply with the relevant legal framework (i.e. GDPR and the “ePrivacy” Directive).

It must also be noted that this guide is of a general nature. Consequently, the recommendations and obligations contained in this document must not be seen as exhaustive. Any assessment must be carried out on a case-by-case basis, and specific applications may require additional measures not included in this guide.

### 1. Summary

In many Member States stakeholders are considering the use of *contact tracing*\* applications to help the population discover whether they have been in contact with a person infected with SARS-CoV-2\*.

The conditions under which such applications would contribute effectively to the management of the pandemic are not yet established. And these conditions would need to be established prior to any implementation of such an app. Yet, it is relevant to provide guidelines bringing relevant information to development teams upstream, so that the protection of personal data can be guaranteed from the early design stage.

It must be noted that this guide is of a general nature. Consequently, the recommendations and obligations contained in this document must not be seen as exhaustive. Any assessment must be carried out on a case-by-case basis, and specific applications may require additional measures not included in this guide. The purpose of this guide is to provide general guidance to designers and implementers of contact tracing applications.

Some criteria might go beyond the strict requirements stemming from the data protection framework. They aim at ensuring the highest level of transparency, in order to favour social acceptance of such contact tracing applications.

To this end, publishers of contact tracing applications should take into account the following criteria:

- ) The use of such an application must be strictly voluntary. It may not condition the access to any rights guaranteed by law. Individuals must have full control over their data at all times, and should be able to choose freely to use such an application.
- ) Contact tracing applications are likely to result in a high risk to the rights and freedoms of natural persons and to require a data protection impact assessment to be conducted prior to their deployment.
- ) Information on the proximity between users of the application can be obtained without locating them. This kind of application does not need, and, hence, should not involve the use of location data.

- ) When a user is diagnosed infected with the SARS-CoV-2 virus, only the persons with whom the user has been in close contact within the epidemiologically relevant retention period for contact tracing, should be informed.
- ) The operation of this type of application might require, depending on the architecture that is chosen, the use of a centralised server. In such a case and in accordance with the principles of data minimisation and data protection by design, the data processed by the centralised server should be limited to the bare minimum:
  - o When a user is diagnosed as infected, information regarding its previous close contacts or the identifiers broadcasted by the user's application can be collected, only with the user's agreement. A verification method needs to be established that allows asserting that the person is indeed infected without identifying the user. Technically this could be achieved by alerting contacts only following the intervention of a healthcare professional, for example by using a special one-time code.
  - o The information stored on the central server should neither allow the controller to identify users diagnosed as infected or having been in contact with those users, nor should it allow the inference of contact patterns not needed for the determination of relevant contacts.
- ) The operation of this type of application requires to broadcast data that is read by devices of other users and listening to these broadcasts:
  - o It is sufficient to exchange pseudonymous identifiers between users' mobile equipment (computers, tablets, connected watches, etc.), for example by broadcasting them (e.g. via the Bluetooth Low Energy technology).
  - o Identifiers must be generated using state-of-the-art cryptographic processes.
  - o Identifiers must be renewed on a regular basis to reduce the risk of physical tracking and linkage attacks.
- ) This type of application must be secured to guarantee safe technical processes. In particular:
  - o The application should not convey to the users information that allows them to infer the identity or the diagnosis of others. The central server must neither identify users, nor infer information about them.

**Disclaimer:** the above principles are related to the claimed purpose of *contact tracing* applications, and to this purpose only, which only aim to automatically inform people potentially exposed to the virus (without having to identify them). The operators of the application and its infrastructure may be controlled by the competent supervisory authority. Following all or part of these guidelines is not necessarily sufficient to ensure a full compliance to the data protection framework.

## 2. Definitions

<b>Contact</b>	For a contact tracing application, a contact is a user who has participated in an interaction with a user confirmed to be a carrier of the virus, and whose duration and distance induce a risk of significant exposure to the virus infection.
----------------	---

	Parameters for duration of exposure and distance between people must be estimated by the health authorities and can be set in the application.
<b>Location data</b>	<p>It refers to all data processed in an electronic communications network or by an electronic communications service indicating the geographical position of the terminal equipment of a user of a publicly available electronic communications service (as defined in the e-Privacy Directive), as well as data from potential other sources, relating to:</p> <ul style="list-style-type: none"> <li>)] the latitude, longitude or altitude of the terminal equipment;</li> <li>)] the direction of travel of the user; or</li> <li>)] the time the location information was recorded.</li> </ul>
<b>Interaction</b>	In the context of the contact tracing application, an interaction is defined as the exchange of information between two devices located in close proximity to each other (in space and time), within the range of the communication technology used (e.g. Bluetooth). This definition excludes the location of the two users of the interaction.
<b>Virus carrier</b>	In this document, we consider virus carriers to be users who have been tested positive for the virus and who have received an official diagnosis from physicians or health centres.
<b>Contact tracing</b>	<p>People who have been in close contact (according to criteria to be defined by epidemiologists) with an individual infected with the virus run a significant risk of also being infected and of infecting others in turn.</p> <p>Contact tracing is a disease control methodology that lists all people who have been in close proximity to a carrier of the virus so as to check whether they are at risk of infection and take the appropriate sanitary measures towards them.</p>

### 3. General

GEN-1	The application must be a complementary tool to traditional contact tracing techniques (notably interviews with infected persons), i.e. be part of a wider public health program. It must be used <u>only</u> up until the point manual contact tracing techniques can manage alone the amount of new infections.
GEN-2	At the latest when "return to normal" is decided by the competent public authorities, a procedure must be put in place to stop the collection of identifiers (global deactivation of the application, instructions to uninstall the application, automatic uninstallation, etc.) and to activate the deletion of all collected data from all databases (mobile applications and servers).

GEN-3	The source code of the application and of its backend must be open, and the technical specifications must be made public, so that any concerned party can audit the code, and where relevant - contribute to improving the code, correcting possible bugs and ensuring transparency in the processing of personal data.
GEN-4	The stages of deployment of the application must make it possible to progressively validate its effectiveness from a public health point of view. An evaluation protocol, specifying indicators allowing to measure the effectiveness of the application, must be defined upstream for this purpose.

#### 4. Purposes

PUR-1	The application must pursue the sole purpose of contact tracing so that people potentially exposed to the SARS-CoV-2 virus can be alerted and taken care of. It must not be used for another purpose.
PUR-2	The application must not be diverted from its primary use for the purpose of monitoring compliance with quarantine or confinement measures and/or social distancing.
PUR-3	The application must not be used to draw conclusions on the location of the users based on their interaction and/or any other means.

#### 5. Functional considerations

FUNC-1	The application must provide a functionality enabling users to be informed that they have been potentially exposed to the virus, this information being based on proximity to an infected user within a window of X days prior to the positive screening test (the X value being defined by the health authorities).
FUNC-2	The application should provide recommendations to users identified as having been potentially exposed to the virus. It should relay instructions regarding the measures they should follow, and they should allow the user to request advises. In such cases, a human intervention would be mandatory.
FUNC-3	The algorithm measuring the risk of infection by taking into account factors of distance and time and thus determining when a contact has to be recorded in the contact tracing list, must be securely tunable to take into account the most recent knowledge on the spread of the virus.
FUNC-4	<b>Users must be informed in case they have been exposed to the virus</b> , or must regularly obtain information on whether or not they have been exposed to the virus, within the incubation period of the virus.
FUNC-5	The application should be interoperable with other applications developed across EU Member States, so that users travelling across different Member States can be efficiently notified.

## 6. Data

DATA-1	The application must be able to broadcast and receive data via proximity communication technologies like Bluetooth Low Energy so that contact tracing can be carried out.
DATA-2	This broadcast data must include cryptographically strong pseudo-random identifiers, generated by and specific to the application.
DATA-3	The risk of collision between pseudo-random identifiers should be sufficiently low.
DATA-4	Pseudo-random identifiers must be renewed regularly, at a frequency sufficient to limit the risk of re-identification, physical tracking or linkage of individuals, by anyone including central server operators, other application users or malicious third parties. These identifiers must be generated by the user's application, possibly based on a seed provided by the central server.
DATA-5	According to the data minimisation principle, the application must not collect data other than what is strictly necessary for the purpose of contact tracing
DATA-6	The application must not collect location data for the purpose of contact tracing. Location data can be processed for the sole purpose of allowing the application to interact with similar applications in other countries and should be limited in precision to what is strictly necessary for this sole purpose.
DATA-7	The application should not collect health data in addition to those that are strictly necessary for the purposes of the app, except on an optional basis and for the sole purpose of assisting in the decision making process of informing the user.
DATA-8	Users must be informed of all personal data that will be collected. This data should be collected only with the user authorization.

## 7. Technical properties

TECH-1	The application should available technologies such as use proximity communication technology (e.g. Bluetooth Low Energy) to detect users in the vicinity of the device running the application.
TECH-2	The application should keep the history of a user's contacts in the equipment, for a predefined limited period of time.
TECH-3	The application may rely on a central server to implement some of its functionalities.

TECH-4	The application must be based on an architecture relying as much as possible on users' devices.
TECH-5	At the initiative of users reported as infected by the virus and after confirmation of their status by an appropriately certified health professional, their contact history or their own identifiers should be transmitted to the central server.

## 8. Security

SEC-1	A mechanism must verify the status of users who report as SARS-CoV-2positive in the application, for example by providing a single-use code linked to a test station or health care professional. If confirmation cannot be obtained in a secure manner, data must not be processed.
SEC-2	The data sent to the central server must be transmitted over a secure channel. The use of notification services provided by OS platform providers should be carefully assessed, and should not lead to disclosing any data to third parties.
SEC-3	Requests must not be vulnerable to tampering by a malicious user
SEC-4	State-of-the-art cryptographic techniques must be implemented to secure exchanges between the application and the server and between applications and as a general rule to protect the information stored in the applications and on the server. Examples of techniques that can be used include for example : symmetric and asymmetric encryption, hash functions, private membership test, private set intersection, Bloom filters, private information retrieval, homomorphic encryption, etc.
SEC-5	The central server must not keep network connection identifiers (e.g., IP addresses) of any users including those who have been positively diagnosed and who transmitted their contacts history or their own identifiers.
SEC-6	In order to avoid impersonation or the creation of fake users, the server must authenticate the application.
SEC-7	The application must authenticate the central server.
SEC-8	The server functionalities should be protected from replay attacks.
SEC-9	The information transmitted by the central server must be signed in order to authenticate its origin and integrity.
SEC-10	Access to all data stored in the central server and not publicly available must be restricted to authorised persons only.
SEC-11	The device's permission manager at the operating system level must only request the permissions necessary to access and use when necessary the communication modules, to store the data in the terminal, and to exchange information with the central server.

## 9. Protection of personal data and privacy of natural persons

*Reminder: the following guidelines concern an application whose sole purpose is contact tracing.*

PRIV-1	Data exchanges must be respectful of the users' privacy (and notably respect the principle of data minimisation).
PRIV-2	The application must not allow users to be directly identified when using the application.
PRIV-3	The application must not allow users' movements to be traced.
PRIV-4	The use of the application should not allow users to learn anything about other users (and notably whether they are virus carriers or not).
PRIV-5	Trust in the central server must be limited. The management of the central server must follow clearly defined governance rules and include all necessary measures to ensure its security. The localization of the central server should allow an effective supervision by the competent supervisory authority.
PRIV-6	A Data Protection Impact Assessment must be carried out and should be made public.
PRIV-7	The application should only reveal to the user whether they have been exposed to the virus, and, if possible without revealing information about other users, the number of times and dates of exposure.
PRIV-8	The information conveyed by the application must not allow users to identify users carrying the virus, nor their movements.
PRIV-9	The information conveyed by the application must not allow health authorities to identify potentially exposed users without their agreement.
PRIV-10	Requests made by the applications to the central server must not reveal anything about the virus carrier.
PRIV-11	Requests made by the applications to the central server must not reveal any unnecessary information about the user, except, possibly, and only when necessary, for their pseudonymous identifiers and their contact list.
PRIV-12	Linkage attacks must not be possible.
PRIV-13	Users must be able to exercise their rights via the application.
PRIV-14	Deletion of the application must result in the deletion of all locally collected data.
PRIV-15	The application should only collect data transmitted by instances of the application or interoperable equivalent applications. No data relating to other applications and/or proximity communication devices shall be collected.
PRIV-16	In order to avoid re-identification by the central server, proxy servers should be implemented. The purpose of these <i>non-colluding servers</i> is to mix the identifiers of several users (both those of virus carriers and those sent by requesters) before sharing them with the central server, so as to prevent the central server from knowing the identifiers (such as IP addresses) of users.
PRIV-17	The application and the server must be carefully developed and configured in order not to collect any unnecessary data (e.g., no identifiers should be included

	in the server logs, etc.) and in order to avoid the use of any third party SDK collecting data for other purposes.
--	--

Most contact tracing applications currently being discussed follow basically two approaches when a user is declared infected: they can either send to a server the history of proximity contacts they have obtained through scanning, or they can send the list of their own identifiers that were broadcasted. The following principles are declined according to these two approaches. While these approaches are discussed here, that does not mean other approaches are not possible or even preferable, for example approaches that implement some form of E2E encryption or apply other security or privacy enhancing technologies.

#### **9.1. Principles that apply only when the application sends to the server a list of contacts:**

CON-1	The central server must collect the contact history of users reported as positive to COVID-19 as a result of voluntary action on their part.
CON-2	The central server must not maintain nor circulate a list of the pseudonymous identifiers of users carrying the virus.
CON-3	Contact history stored on the central server must be deleted once users are notified of their proximity with a positively diagnosed person.
CON-4	Except when the user detected as positive shares his contact history with the central server or when the user makes a request to the server to find out his potential exposure to the virus, no data must leave the user's equipment.
CON-5	Any identifier included in the local history must be deleted after X days from its collection (the X value being defined by the health authorities).
CON-6	Contact histories submitted by distinct users should not further be processed e.g. cross-correlated to build global proximity maps.
CON-7	Data in server logs must be minimised and must comply with data protection requirements

#### **9.2. Principles that apply only when the application sends to a server a list of its own identifiers:**

ID-1	The central server must collect the identifiers broadcast by the application of users reported as positive to COVID-19, as a result of voluntary action on their part.
ID-2	The central server must not maintain nor circulate the contact history of users carrying the virus.
ID-3	Identifiers stored on the central server must be deleted once they were distributed to the other applications.
ID-4	Except when the user detected as positive shares his identifiers with the central server, no data must leave the user's equipment or when the user makes a

	request to the server to find out his potential exposure to the virus, no data must leave the user's equipment.
ID-5	Data in server logs must be minimised and must comply with data protection requirements

# Guidelines



**Guidelines 05/2020 on consent under Regulation 2016/679**

**Version 1.1**

**Adopted on 4 May 2020**

## Version history

Version 1.1	13 May 2020	Formatting corrections
Version 1.0	4 May 2020	Adoption of the Guidelines

## Table of contents

0	Preface.....	4
1	Introduction.....	4
2	Consent in Article 4(11) of the GDPR .....	6
3	Elements of valid consent .....	7
3.1	Free / freely given .....	7
3.1.1	Imbalance of power.....	8
3.1.2	Conditionality .....	10
3.1.3	Granularity.....	12
3.1.4	Detriment .....	13
3.2	Specific.....	13
3.3	Informed.....	15
3.3.1	Minimum content requirements for consent to be ‘informed’ .....	15
3.3.2	How to provide information.....	16
3.4	Unambiguous indication of wishes .....	18
4	Obtaining explicit consent.....	20
5	Additional conditions for obtaining valid consent .....	22
5.1	Demonstrate consent.....	22
5.2	Withdrawal of consent.....	23
6	Interaction between consent and other lawful grounds in Article 6 GDPR .....	25
7	Specific areas of concern in the GDPR .....	25
7.1	Children (Article 8) .....	25
7.1.1	Information society service .....	26
7.1.2	Offered directly to a child.....	27
7.1.3	Age.....	27
7.1.4	Children’s consent and parental responsibility.....	28
7.2	Scientific research .....	30
7.3	Data subject’s rights .....	32
8	Consent obtained under Directive 95/46/EC.....	32

# The European Data Protection Board

Having regard to Article 70 (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”),

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<sup>1</sup>,

Having regard to Article 12 and Article 22 of its Rules of Procedure,

Having regard to the Article 29 Working Party Guidelines on consent under Regulation 2016/679, WP259 rev.01,

## HAS ADOPTED THE FOLLOWING GUIDELINES

### 0 PREFACE

On 10 April 2018 the Article 29 Working Party adopted its Guidelines on consent under Regulation 2016/679 (WP259.01), which were endorsed by the European Data Protection Board (hereinafter “EDPB”) at its first Plenary meeting. This document is a slightly updated version of those Guidelines. Any reference to the WP29 Guidelines on consent (WP259 rev.01) should from now on be interpreted as a reference to these guidelines.

The EDPB has noticed that there was a need for further clarifications, specifically regarding two questions:

- 1 The validity of consent provided by the data subject when interacting with so-called “cookie walls”;
- 2 The example 16 on scrolling and consent.

The paragraphs concerning these two issues have been revised and updated, while the rest of the document was left unchanged, except for editorial changes. The revision concerns, more specifically:

- ) Section on Conditionality (paragraphs 38 - 41).
- ) Section on Unambiguous indication of wishes (paragraph 86)

### 1 INTRODUCTION

1. These Guidelines provide a thorough analysis of the notion of consent in Regulation 2016/679, the General Data Protection Regulation (hereafter: GDPR). The concept of consent as used in the Data

---

<sup>1</sup> References to “Member States” made throughout this document should be understood as references to “EEA Member States”.

Protection Directive (hereafter: Directive 95/46/EC) and in the e-Privacy Directive to date, has evolved. The GDPR provides further clarification and specification of the requirements for obtaining and demonstrating valid consent. These Guidelines focus on these changes, providing practical guidance to ensure compliance with the GDPR and building upon the Article 29 Working Party Opinion 15/2011 on consent. The obligation is on controllers to innovate to find new solutions that operate within the parameters of the law and better support the protection of personal data and the interests of data subjects.

2. Consent remains one of six lawful bases to process personal data, as listed in Article 6 of the GDPR.<sup>2</sup> When initiating activities that involve processing of personal data, a controller must always take time to consider what would be the appropriate lawful ground for the envisaged processing.
3. Generally, consent can only be an appropriate lawful basis if a data subject is offered control and is offered a genuine choice with regard to accepting or declining the terms offered or declining them without detriment. When asking for consent, a controller has the duty to assess whether it will meet all the requirements to obtain valid consent. If obtained in full compliance with the GDPR, consent is a tool that gives data subjects control over whether or not personal data concerning them will be processed. If not, the data subject's control becomes illusory and consent will be an invalid basis for processing, rendering the processing activity unlawful.<sup>3</sup>
4. The existing Article 29 Working Party (WP29) Opinions on consent<sup>4</sup> remain relevant, where consistent with the new legal framework, as the GDPR codifies existing WP29 guidance and general good practice and most of the key elements of consent remain the same under the GDPR. Therefore, in this document, the EDPB expands upon and completes earlier Article 29 Working Party Opinions on specific topics that include reference to consent under Directive 95/46/EC, rather than replacing them.
5. As the WP29 stated in its Opinion 15/2011 on the definition on consent, inviting people to accept a data processing operation should be subject to rigorous requirements, since it concerns the fundamental rights of data subjects and the controller wishes to engage in a processing operation that would be unlawful without the data subject's consent.<sup>5</sup> The crucial role of consent is underlined by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. Furthermore, obtaining consent also does not negate or in any way diminish the controller's obligations to observe the principles of processing enshrined in the GDPR, especially Article 5 of the GDPR with regard to fairness, necessity and proportionality, as well as data quality. Even if the processing of personal data is based on consent of the data subject, this would not legitimise collection of data, which is not necessary in relation to a specified purpose of processing and be fundamentally unfair.<sup>6</sup>

---

<sup>2</sup> Article 9 GDPR provides a list of possible exemptions to the ban on processing special categories of data. One of the exemptions listed is the situation where the data subject provides explicit consent to the use of this data.

<sup>3</sup> See also Article 29 Working Party Opinion 15/2011 on the definition of consent (WP 187), pp. 6-8, and/or Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217), pp. 9, 10, 13 and 14.

<sup>4</sup> Most notably, Opinion 15/2011 on the definition of consent (WP 187).

<sup>5</sup> Opinion 15/2011, page on the definition of consent (WP 187), p. 8.

<sup>6</sup> See also Opinion 15/2011 on the definition of consent (WP 187), and Article 5 GDPR.

6. Meanwhile, the EDPB is aware of the review of the ePrivacy Directive (2002/58/EC). The notion of consent in the draft ePrivacy Regulation remains linked to the notion of consent in the GDPR.<sup>7</sup> Organisations are likely to need consent under the ePrivacy instrument for most online marketing messages or marketing calls, and online tracking methods including by the use of cookies or apps or other software. The EDPB has already provided recommendations and guidance to the European legislator on the Proposal for a Regulation on ePrivacy.<sup>8</sup>
7. With regard to the existing e-Privacy Directive, the EDPB notes that references to the repealed Directive 95/46/EC shall be construed as references to the GDPR.<sup>9</sup> This also applies to references to consent in the current Directive 2002/58/EC, as the ePrivacy Regulation will not (yet) be in force from 25 May 2018. According to Article 95 GDPR, additional obligations in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks shall not be imposed insofar the e-Privacy Directive imposes specific obligations with the same objective. The EDPB notes that the requirements for consent under the GDPR are not considered to be an ‘additional obligation’, but rather as preconditions for lawful processing. Therefore, the GDPR conditions for obtaining valid consent are applicable in situations falling within the scope of the e-Privacy Directive.

## 2 CONSENT IN ARTICLE 4(11) OF THE GDPR

8. Article 4(11) of the GDPR defines consent as: “any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.”
9. The basic concept of consent remains similar to that under the Directive 95/46/EC and consent is one of the lawful grounds on which personal data processing has to be based, pursuant to Article 6 of the GDPR.<sup>10</sup> Besides the amended definition in Article 4(11), the GDPR provides additional guidance in Article 7 and in recitals 32, 33, 42, and 43 as to how the controller must act to comply with the main elements of the consent requirement.

---

<sup>7</sup> According to Article 9 of the proposed ePrivacy Regulation, the definition of and the conditions for consent provided for in Articles 4(11) and Article 7 of the GDPR apply.

<sup>8</sup> See [EDPB statement on ePrivacy - 25/05/2018](#) and [EDPB Statement 3/2019 on an ePrivacy regulation](#).

<sup>9</sup> See Article 94 GDPR.

<sup>10</sup> Consent was defined in Directive 95/46/EC as “any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed” which must be ‘unambiguously given’ in order to make the processing of personal data legitimate (Article 7(a) of Directive 95/46/EC)). See WP29 Opinion 15/2011 on the definition of consent (WP 187) for examples on the appropriateness of consent as lawful basis. In this Opinion, WP29 has provided guidance to distinguish where consent is an appropriate lawful basis from those where relying on the legitimate interest ground (perhaps with an opportunity to opt out) is sufficient or a contractual relation would be recommended. See also WP29 Opinion 06/2014, paragraph III.1.2, p. 14 and further. Explicit consent is also one of the exemptions to the prohibition on the processing of special categories of data: See Article 9 GDPR.

10. Finally, the inclusion of specific provisions and recitals on the withdrawal of consent confirms that consent should be a reversible decision and that there remains a degree of control on the side of the data subject.

### 3 ELEMENTS OF VALID CONSENT

11. Article 4(11) of the GDPR stipulates that consent of the data subject means any:
  - ✓ freely given,
  - ✓ specific,
  - ✓ informed and
  - ✓ unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

12. In the sections below, it is analysed to what extent the wording of Article 4(11) requires controllers to change their consent requests/forms, in order to ensure compliance with the GDPR.<sup>11</sup>

#### 3.1 Free / freely given<sup>12</sup>

13. The element “free” implies real choice and control for data subjects. As a general rule, the GDPR prescribes that if the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid.<sup>13</sup> If consent is bundled up as a non-negotiable part of terms and conditions it is presumed not to have been freely given. Accordingly, consent will not be considered to be free if the data subject is unable to refuse or withdraw his or her consent without detriment.<sup>14</sup> The notion of imbalance between the controller and the data subject is also taken into consideration by the GDPR.
14. When assessing whether consent is freely given, one should also take into account the specific situation of tying consent into contracts or the provision of a service as described in Article 7(4). Article 7(4) has been drafted in a non-exhaustive fashion by the words “inter alia”, meaning that there may be a range of other situations, which are caught by this provision. In general terms, any element of

---

<sup>11</sup> For guidance with regard to ongoing processing activities based on consent in Directive 95/46, see chapter 7 of this document and recital 171 of the GDPR.

<sup>12</sup> In several opinions, the Article 29 Working Party has explored the limits of consent in situations where it cannot be freely given. This was notably the case in its Opinion 15/2011 on the definition of consent (WP 187), Working Document on the processing of personal data relating to health in electronic health records (WP 131), Opinion 8/2001 on the processing of personal data in the employment context (WP48), and Second opinion 4/2009 on processing of data by the World Anti-Doping Agency (WADA) (International Standard for the Protection of Privacy and Personal Information, on related provisions of the WADA Code and on other privacy issues in the context of the fight against doping in sport by WADA and (national) anti-doping organizations (WP 162).

<sup>13</sup> See Opinion 15/2011 on the definition of consent (WP187), p. 12.

<sup>14</sup> See Recitals 42, 43 GDPR and WP29 Opinion 15/2011 on the definition of consent, adopted on 13 July 2011, (WP 187), p. 12.

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.

15. Example 1: A mobile app for photo editing asks its users to have their GPS localisation activated for the use of its services. The app also tells its users it will use the collected data for behavioural advertising purposes. Neither geolocation or online behavioural advertising are necessary for the provision of the photo editing service and go beyond the delivery of the core service provided. Since users cannot use the app without consenting to these purposes, the consent cannot be considered as being freely given.

### 3.1.1 Imbalance of power

16. Recital 43<sup>15</sup> clearly indicates that it is unlikely that **public authorities** can rely on consent for processing as whenever the controller is a public authority, there is often a clear imbalance of power in the relationship between the controller and the data subject. It is also clear in most cases that the data subject will have no realistic alternatives to accepting the processing (terms) of this controller. The EDPB considers that there are other lawful bases that are, in principle, more appropriate to the activity of public authorities.<sup>16</sup>
17. Without prejudice to these general considerations, the use of consent as a lawful basis for data processing by public authorities is not totally excluded under the legal framework of the GDPR. The following examples show that the use of consent can be appropriate under certain circumstances.

18. Example 2: A local municipality is planning road maintenance works. As the road works may disrupt traffic for a long time, the municipality offers its citizens the opportunity to subscribe to an email list to receive updates on the progress of the works and on expected delays. The municipality makes clear that there is no obligation to participate and asks for consent to use email addresses for this (exclusive) purpose. Citizens that do not consent will not miss out on any core service of the municipality or the exercise of any right, so they are able to give or refuse their consent to this use of data freely. All information on the road works will also be available on the municipality's website.
19. Example 3: An individual who owns land needs certain permits from both her local municipality and from the provincial government under which the municipality resides. Both public bodies require the same information for issuing their permit, but are not accessing each other's databases. Therefore, both ask for the same information and the land owner sends out her details to both public bodies. The municipality and the provincial authority ask for her consent to merge the files, to avoid duplicate procedures and correspondence. Both public bodies ensure that this is optional and that the permit requests will still be processed separately if she decides not to consent to the merger of her data. The land owner is able to give consent to the authorities for the purpose of merging the files freely.

---

<sup>15</sup> Recital 43 GDPR states: "*In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. (...)*".

<sup>16</sup> See Article 6 GDPR, notably paragraphs (1c) and (1e).

20. Example 4: A public school asks students for consent to use their photographs in a printed student magazine. Consent in these situations would be a genuine choice as long as students will not be denied education or services and could refuse the use of these photographs without any detriment.<sup>17</sup>
21. An imbalance of power also occurs in the **employment** context.<sup>18</sup> Given the dependency that results from the employer/employee relationship, it is unlikely that the data subject is able to deny his/her employer consent to data processing without experiencing the fear or real risk of detrimental effects as a result of a refusal. It is unlikely that an employee would be able to respond freely to a request for consent from his/her employer to, for example, activate monitoring systems such as camera observation in a workplace, or to fill out assessment forms, without feeling any pressure to consent.<sup>19</sup> Therefore, the EDPB deems it problematic for employers to process personal data of current or future employees on the basis of consent as it is unlikely to be freely given. For the majority of such data processing at work, the lawful basis cannot and should not be the consent of the employees (Article 6(1)(a)) due to the nature of the relationship between employer and employee.<sup>20</sup>
22. However, this does not mean that employers can never rely on consent as a lawful basis for processing. There may be situations when it is possible for the employer to demonstrate that consent actually is freely given. Given the imbalance of power between an employer and its staff members, employees can only give free consent in exceptional circumstances, when it will have no adverse consequences at all whether or not they give consent.<sup>21</sup>
23. Example 5: A film crew is going to be filming in a certain part of an office. The employer asks all the employees who sit in that area for their consent to be filmed, as they may appear in the background of the video. Those who do not want to be filmed are not penalised in any way but instead are given equivalent desks elsewhere in the building for the duration of the filming.
24. Imbalances of power are not limited to public authorities and employers, they may also occur in other situations. As highlighted by the WP29 in several Opinions, consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences (e.g. substantial extra costs) if he/she does not consent. Consent will not be free in cases where there is any element of compulsion, pressure or inability to exercise free will.

---

<sup>17</sup> For the purposes of this example, a public school means a publicly funded school or any educational facility that qualifies as a public authority or body by national law.

<sup>18</sup> See also Article 88 GDPR, where the need for protection of the specific interests of employees is emphasised and a possibility for derogations in Member State law is created. See also Recital 155.

<sup>19</sup> See Opinion 15/2011 on the definition of consent (WP 187), pp. 12-14 , Opinion 8/2001 on the processing of personal data in the employment context (WP 48), Chapter 10, Working document on the surveillance of electronic communications in the workplace (WP 55), paragraph 4.2 and Opinion 2/2017 on data processing at work (WP 249), paragraph 6.2.

<sup>20</sup> See Opinion 2/2017 on data processing at work, page 6-7.

<sup>21</sup> See also Opinion 2/2017 on data processing at work (WP249), paragraph 6.2.

### 3.1.2 Conditionality

25. To assess whether consent is freely given, Article 7(4) GDPR plays an important role.<sup>22</sup>
26. Article 7(4) GDPR indicates that, *inter alia*, the situation of “bundling” consent with acceptance of terms or conditions, or “tying” the provision of a contract or a service to a request for consent to process personal data that are not necessary for the performance of that contract or service, is considered highly undesirable. If consent is given in this situation, it is presumed to be not freely given (recital 43). Article 7(4) seeks to ensure that the purpose of personal data processing is not disguised nor bundled with the provision of a contract or a service for which these personal data are not necessary. In doing so, the GDPR ensures that the processing of personal data for which consent is sought cannot become directly or indirectly the counter-performance of a contract. The two lawful bases for the lawful processing of personal data, i.e. consent and contract cannot be merged and blurred.
27. Compulsion to agree with the use of personal data additional to what is strictly necessary limits data subject’s choices and stands in the way of free consent. As data protection law is aiming at the protection of fundamental rights, an individual’s control over their personal data is essential and there is a strong presumption that consent to the processing of personal data that is unnecessary, cannot be seen as a mandatory consideration in exchange for the performance of a contract or the provision of a service.
28. Hence, whenever a request for consent is tied to the performance of a contract by the controller, a data subject that does not wish to make his/her personal data available for processing by the controller runs the risk to be denied services they have requested.
29. To assess whether such a situation of bundling or tying occurs, it is important to determine what the scope of the contract is and what data would be necessary for the performance of that contract.
30. According to Opinion 06/2014 of WP29, the term “necessary for the performance of a contract” needs to be interpreted strictly. The processing must be necessary to fulfil the contract with each individual data subject. This may include, for example, processing the address of the data subject so that goods purchased online can be delivered, or processing credit card details in order to facilitate payment. In the employment context, this ground may allow, for example, the processing of salary information and bank account details so that wages can be paid.<sup>23</sup> There needs to be a direct and objective link between the processing of the data and the purpose of the execution of the contract.
31. If a controller seeks to process personal data that are in fact necessary for the performance of a contract, then consent is not the appropriate lawful basis.<sup>24</sup>

---

<sup>22</sup> Article 7(4) GDPR: “*When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.*” See also Recital 43 GDPR, that states: “[...] Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent, despite such consent not being necessary for such performance.”

<sup>23</sup> For more information and examples, see Opinion 06/2014 on the notion of legitimate interest of the data controller under Article 7 of Directive 95/46/EC, adopted by WP29 on 9 April 2014, p. 16-17. (WP 217).

<sup>24</sup> The appropriate lawful basis could then be Article 6(1)(b) (contract).

32. Article 7(4) is only relevant where the requested data are **not** necessary for the performance of the contract, (including the provision of a service), and the performance of that contract is made conditional on the obtaining of these data on the basis of consent. Conversely, if processing is necessary to perform the contract (including to provide a service), then Article 7(4) does not apply.

33. Example 6: A bank asks customers for consent to allow third parties to use their payment details for direct marketing purposes. This processing activity is not necessary for the performance of the contract with the customer and the delivery of ordinary bank account services. If the customer's refusal to consent to this processing purpose would lead to the denial of banking services, closure of the bank account, or, depending on the case, an increase of the fee, consent cannot be freely given.

34. The choice of the legislator to highlight conditionality, amongst others, as a presumption of a lack of freedom to consent, demonstrates that the occurrence of conditionality must be carefully scrutinized. The term "utmost account" in Article 7(4) suggests that special caution is needed from the controller when a contract (which could include the provision of a service) has a request for consent to process personal data tied to it.

35. As the wording of Article 7(4) is not construed in an absolute manner, there might be very limited space for cases where this conditionality would not render the consent invalid. However, the word "presumed" in Recital 43 clearly indicates that such cases will be highly exceptional.

36. In any event, the burden of proof in Article 7(4) is on the controller.<sup>25</sup> This specific rule reflects the general principle of accountability, which runs throughout the GDPR. However, when Article 7(4) applies, it will be more difficult for the controller to prove that consent was given freely by the data subject.<sup>26</sup>

37. The controller could argue that his organisation offers data subjects genuine choice if they were able to choose between a service that includes consenting to the use of personal data for additional purposes on the one hand, and an equivalent service offered by the same controller that does not involve consenting to data use for additional purposes on the other hand. As long as there is a possibility to have the contract performed or the contracted service delivered by this controller without consenting to the other or additional data use in question, this means there is no longer a conditional service. However, both services need to be genuinely equivalent.

38. The EDPB considers that consent cannot be considered as freely given if a controller argues that a choice exists between its service that includes consenting to the use of personal data for additional purposes on the one hand, and an equivalent service offered by a different controller on the other hand. In such a case, the freedom of choice would be made dependent on what other market players do and whether an individual data subject would find the other controller's services genuinely

---

<sup>25</sup> See also Article 7(1) GDPR, which states that the controller needs to demonstrate that the data subject's agreement was freely given.

<sup>26</sup> To some extent, the introduction of this paragraph is a codification of existing WP29 guidance. As described in Opinion 15/2011, when a data subject is in a situation of dependence on the data controller – due to the nature of the relationship or to special circumstances – there may be a strong presumption that freedom to consent is limited in such contexts (e.g. in an employment relationship or if the collection of data is performed by a public authority). With Article 7(4) in force, it will be more difficult for the controller to prove that consent was given freely by the data subject. See: Article 29 Working Party Opinion 15/2011 on the definition of consent (WP 187), pp. 12-17.

equivalent. It would furthermore imply an obligation for controllers to monitor market developments to ensure the continued validity of consent for their data processing activities, as a competitor may alter its service at a later stage. Hence, using this argument means a consent relying on an alternative option offered by a third party fails to comply with the GDPR, meaning that a service provider cannot prevent data subjects from accessing a service on the basis that they do not consent.

39. In order for consent to be freely given, access to services and functionalities must not be made conditional on the consent of a user to the storing of information, or gaining of access to information already stored, in the terminal equipment of a user (so called cookie walls)<sup>27</sup>.
40. Example 6a: A website provider puts into place a script that will block content from being visible except for a request to accept cookies and the information about which cookies are being set and for what purposes data will be processed. There is no possibility to access the content without clicking on the “Accept cookies” button. Since the data subject is not presented with a genuine choice, its consent is not freely given.
41. This does not constitute valid consent, as the provision of the service relies on the data subject clicking the “Accept cookies” button. It is not presented with a genuine choice.

### 3.1.3 Granularity

42. A service may involve multiple processing operations for more than one purpose. In such cases, the data subjects should be free to choose which purpose they accept, rather than having to consent to a bundle of processing purposes. In a given case, several consents may be warranted to start offering a service, pursuant to the GDPR.
43. Recital 43 clarifies that consent is presumed not to be freely given if the process/procedure for obtaining consent does not allow data subjects to give separate consent for personal data processing operations respectively (e.g. only for some processing operations and not for others) despite it being appropriate in the individual case. Recital 32 states, *“Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them”*.
44. If the controller has conflated several purposes for processing and has not attempted to seek separate consent for each purpose, there is a lack of freedom. This granularity is closely related to the need of consent to be specific, as discussed in section 3.2 further below. When data processing is done in pursuit of several purposes, the solution to comply with the conditions for valid consent lies in granularity, i.e. the separation of these purposes and obtaining consent for each purpose.
45. Example 7: Within the same consent request a retailer asks its customers for consent to use their data to send them marketing by email and also to share their details with other companies within their group. This consent is not granular as there is no separate consents for these two separate purposes, therefore the consent will not be valid. In this case, a specific consent should be collected to send the contact details to commercial partners. Such specific consent will be deemed valid for each partner (see also section 3.3.1), whose identity has been provided to the data subject at the time of the collection of his or her consent, insofar as it is sent to them for the same purpose (in this example: a marketing purpose).

---

<sup>27</sup> As clarified above, the GDPR conditions for obtaining valid consent are applicable in situations falling within the scope of the e-Privacy Directive.

### 3.1.4 Detriment

46. The controller needs to demonstrate that it is possible to refuse or withdraw consent without detriment (recital 42). For example, the controller needs to prove that withdrawing consent does not lead to any costs for the data subject and thus no clear disadvantage for those withdrawing consent.
  47. Other examples of detriment are deception, intimidation, coercion or significant negative consequences if a data subject does not consent. The controller should be able to prove that the data subject had a free or genuine choice about whether to consent and that it was possible to withdraw consent without detriment.
  48. If a controller is able to show that a service includes the possibility to withdraw consent without any negative consequences e.g. without the performance of the service being downgraded to the detriment of the user, this may serve to show that the consent was given freely. The GDPR does not preclude all incentives but the onus would be on the controller to demonstrate that consent was still freely given in all the circumstances.
49. Example 8: When downloading a lifestyle mobile app, the app asks for consent to access the phone's accelerometer. This is not necessary for the app to work, but it is useful for the controller who wishes to learn more about the movements and activity levels of its users. When the user later revokes that consent, she finds out that the app now only works to a limited extent. This is an example of detriment as meant in Recital 42, which means that consent was never validly obtained (and thus, the controller needs to delete all personal data about users' movements collected this way).
  50. Example 9: A data subject subscribes to a fashion retailer's newsletter with general discounts. The retailer asks the data subject for consent to collect more data on shopping preferences to tailor the offers to his or her preferences based on shopping history or a questionnaire that is voluntary to fill out. When the data subject later revokes consent, he or she will receive non-personalised fashion discounts again. This does not amount to detriment as only the permissible incentive was lost.
51. Example 10: A fashion magazine offers readers access to buy new make-up products before the official launch.
  52. The products will shortly be made available for sale, but readers of this magazine are offered an exclusive preview of these products. In order to enjoy this benefit, people must give their postal address and agree to subscription on the mailing list of the magazine. The postal address is necessary for shipping and the mailing list is used for sending commercial offers for products such as cosmetics or t-shirts year round.
  53. The company explains that the data on the mailing list will only be used for sending merchandise and paper advertising by the magazine itself and is not to be shared with any other organisation.
  54. In case the reader does not want to disclose their address for this reason, there is no detriment, as the products will be available to them anyway.

### 3.2 Specific

55. Article 6(1)(a) confirms that the consent of the data subject must be given in relation to "one or more specific" purposes and that a data subject has a choice in relation to each of them.<sup>28</sup> The requirement

---

<sup>28</sup> Further guidance on the determination of 'purposes' can be found in Opinion 3/2013 on purpose limitation (WP 203).

that consent must be '*specific*' aims to ensure a degree of user control and transparency for the data subject. This requirement has not been changed by the GDPR and remains closely linked to the requirement of '*informed*' consent. At the same time, it must be interpreted in line with the requirement for '*granularity*' to obtain '*free*' consent.<sup>29</sup> In sum, to comply with the element of '*specific*' the controller must apply:

- i Purpose specification as a safeguard against function creep,
- ii Granularity in consent requests, and
- iii Clear separation of information related to obtaining consent for data processing activities from information about other matters.

56. **Ad. (i):** Pursuant to Article 5(1)(b) GDPR, obtaining valid consent is always preceded by the determination of a specific, explicit and legitimate purpose for the intended processing activity.<sup>30</sup> The need for specific consent in combination with the notion of purpose limitation in Article 5(1)(b) functions as a safeguard against the gradual widening or blurring of purposes for which data is processed, after a data subject has agreed to the initial collection of the data. This phenomenon, also known as function creep, is a risk for data subjects, as it may result in unanticipated use of personal data by the controller or by third parties and in loss of data subject control.
57. If the controller is relying on Article 6(1)(a), data subjects must always give consent for a specific processing purpose.<sup>31</sup> In line with the concept of *purpose limitation*, Article 5(1)(b) and recital 32, consent may cover different operations, as long as these operations serve the same purpose. It goes without saying that specific consent can only be obtained when data subjects are specifically informed about the intended purposes of data use concerning them.
58. Notwithstanding the provisions on compatibility of purposes, consent must be specific to the purpose. Data subjects will give their consent with the understanding that they are in control and their data will only be processed for those specified purposes. If a controller processes data based on consent and wishes to process the data for another purpose, too, that controller needs to seek additional consent for this other purpose unless there is another lawful basis, which better reflects the situation.

59. Example 11: A cable TV network collects subscribers' personal data, based on their consent, to present them with personal suggestions for new movies they might be interested in based on their viewing habits. After a while, the TV network decides it would like to enable third parties to send (or display) targeted advertising on the basis of the subscriber's viewing habits. Given this new purpose, new consent is needed.

60. **Ad. (ii):** Consent mechanisms must not only be granular to meet the requirement of '*free*', but also to meet the element of '*specific*'. This means, a controller that seeks consent for various different

---

<sup>29</sup> Recital 43 GDPR states that separate consent for different processing operations will be needed wherever appropriate.

Granular consent options should be provided to allow data subjects to consent separately to separate purposes.

<sup>30</sup> See WP 29 Opinion 3/2013 on purpose limitation (WP 203), p. 16, : "*For these reasons, a purpose that is vague or general, such as for instance 'improving users' experience', 'marketing purposes', 'IT-security purposes' or 'future research' will - without more detail - usually not meet the criteria of being 'specific'.*"

<sup>31</sup> This is consistent with WP29 Opinion 15/2011 on the definition of consent (WP 187), for example on p. 17.

purposes should provide a separate opt-in for each purpose, to allow users to give specific consent for specific purposes.

61. **Ad. (iii):** Lastly, controllers should provide specific information with each separate consent request about the data that are processed for each purpose, in order to make data subjects aware of the impact of the different choices they have. Thus, data subjects are enabled to give specific consent. This issue overlaps with the requirement that controllers must provide clear information, as discussed in paragraph 3.3. below.

### 3.3 Informed

62. The GDPR reinforces the requirement that consent must be informed. Based on Article 5 of the GDPR, the requirement for transparency is one of the fundamental principles, closely related to the principles of fairness and lawfulness. Providing information to data subjects prior to obtaining their consent is essential in order to enable them to make informed decisions, understand what they are agreeing to, and for example exercise their right to withdraw their consent. If the controller does not provide accessible information, user control becomes illusory and consent will be an invalid basis for processing.
63. The consequence of not complying with the requirements for informed consent is that consent will be invalid and the controller may be in breach of Article 6 of the GDPR.

#### 3.3.1 Minimum content requirements for consent to be ‘informed’

64. For consent to be informed, it is necessary to inform the data subject of certain elements that are crucial to make a choice. Therefore, the EDPB is of the opinion that at least the following information is required for obtaining valid consent:
- i. the controller’s identity,<sup>32</sup>
  - ii. the purpose of each of the processing operations for which consent is sought,<sup>33</sup>
  - iii. what (type of) data will be collected and used,<sup>34</sup>
  - iv. the existence of the right to withdraw consent,<sup>35</sup>
  - v. information about the use of the data for automated decision-making in accordance with Article 22 (2)(c)<sup>36</sup> where relevant, and

---

<sup>32</sup> See also Recital 42 GDPR: “ [...]For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended.[...].”

<sup>33</sup> Again, see Recital 42 GDPR.

<sup>34</sup> See also WP29 Opinion 15/2011 on the definition of consent (WP 187) pp.19-20.

<sup>35</sup> See Article 7(3) GDPR.

<sup>36</sup> See also WP29 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251), paragraph IV.B, p. 20 onwards.

- vi. on the possible risks of data transfers due to absence of an adequacy decision and of appropriate safeguards as described in Article 46.<sup>37</sup>
65. With regard to item (i) and (iii), the EDPB notes that in a case where the consent sought is to be relied upon by multiple (joint) controllers or if the data is to be transferred to or processed by other controllers who wish to rely on the original consent, these organisations should all be named. Processors do not need to be named as part of the consent requirements, although to comply with Articles 13 and 14 of the GDPR, controllers will need to provide a full list of recipients or categories of recipients including processors. To conclude, the EDPB notes that depending on the circumstances and context of a case, more information may be needed to allow the data subject to genuinely understand the processing operations at hand.
- 3.3.2 How to provide information**
66. The GDPR does not prescribe the form or shape in which information must be provided in order to fulfil the requirement of informed consent. This means valid information may be presented in various ways, such as written or oral statements, or audio or video messages. However, the GDPR puts several requirements for informed consent in place, predominantly in Article 7(2) and Recital 32. This leads to a higher standard for the clarity and accessibility of the information.
67. When seeking consent, controllers should ensure that they use clear and plain language in all cases. This means a message should be easily understandable for the average person and not only for lawyers. Controllers cannot use long privacy policies that are difficult to understand or statements full of legal jargon. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form. This requirement essentially means that information relevant for making informed decisions on whether or not to consent may not be hidden in general terms and conditions.<sup>38</sup>
68. A controller must ensure that consent is provided on the basis of information that allows the data subjects to easily identify who the controller is and to understand what they are agreeing to. The controller must clearly describe the purpose for data processing for which consent is requested.<sup>39</sup>
69. Other specific guidance on the accessibility has been provided in the WP29 guidelines on transparency. If consent is to be given by electronic means, the request must be clear and concise. Layered and granular information can be an appropriate way to deal with the two-fold obligation of being precise and complete on the one hand and understandable on the other hand.
70. A controller must assess what kind of audience it is that provides personal data to their organisation. For example, in case the targeted audience includes data subjects that are underage, the controller is expected to make sure information is understandable for minors.<sup>40</sup> After identifying their audience,

<sup>37</sup> Pursuant to Article 49 (1)(a), specific information is required about the absence of safeguards described in Article 46, when explicit consent is sought. See also WP29 Opinion 15/2011 on the definition of consent (WP 187)p. 19.

<sup>38</sup> The declaration of consent must be named as such. Drafting, such as “I know that...” does not meet the requirement of clear language.

<sup>39</sup> See Articles 4(11) and 7(2) GDPR.

<sup>40</sup> See also Recital 58 regarding information understandable for children.

controllers must determine what information they should provide and, subsequently how they will present the information to data subjects.

71. Article 7(2) addresses pre-formulated written declarations of consent, which also concern other matters. When consent is requested as part of a (paper) contract, the request for consent should be clearly distinguishable from the other matters. If the paper contract includes many aspects that are unrelated to the question of consent to the use of personal data, the issue of consent should be dealt with in a way that clearly stands out, or in a separate document. Likewise, if consent is requested by electronic means, the consent request has to be separate and distinct, it cannot simply be a paragraph within terms and conditions, pursuant to Recital 32.<sup>41</sup> To accommodate for small screens or situations with restricted room for information, a layered way of presenting information can be considered, where appropriate, to avoid excessive disturbance of user experience or product design.
72. A controller that relies on consent of the data subject must also deal with the separate information duties laid down in Articles 13 and 14 in order to be compliant with the GDPR. In practice, compliance with the information duties and compliance with the requirement of informed consent may lead to an integrated approach in many cases. However, this section is written in the understanding that valid “informed” consent can exist, even when not all elements of Articles 13 and/or 14 are mentioned in the process of obtaining consent (these points should of course be mentioned in other places, such as the privacy notice of a company). WP29 has issued separate guidelines on the requirement of transparency.
73. Example 12: Company X is a controller that received complaints that it is unclear to data subjects for what purposes of data use they are asked to consent to. The company sees the need to verify whether its information in the consent request is understandable for data subjects. X organises voluntary test panels of specific categories of its customers and presents new updates of its consent information to these test audiences before communicating it externally. The selection of the panel respects the principle of independence and is made on the basis of standards ensuring a representative, non-biased outcome. The panel receives a questionnaire and indicates what they understood of the information and how they would score it in terms of understandable and relevant information. The controller continues testing until the panels indicate that the information is understandable. X draws up a report of the test and keeps this available for future reference. This example shows a possible way for X to demonstrate that data subjects were receiving clear information before consenting to personal data processing by X.
74. Example 13: A company engages in data processing on the basis of consent. The company uses a layered privacy notice that includes a consent request. The company discloses all basic details of the controller and the data processing activities envisaged.<sup>42</sup> However, the company does not indicate how their data protection officer can be contacted in the first information layer of the notice. For the purposes of having a valid lawful basis as meant in Article 6, this controller obtained valid “informed”

---

<sup>41</sup> See also Recital 42 and Directive 93/13/EC, notably Article 5 (plain intelligible language and in case of doubt, the interpretation will be in favour of consumer) and Article 6 (invalidity of unfair terms, contract continues to exist without these terms only if still sensible, otherwise the whole contract is invalid).

<sup>42</sup> Note that when the identity of the controller or the purpose of the processing is not apparent from the first information layer of the layered privacy notice (and are located in further sub-layers), it will be difficult for the data controller to demonstrate that the data subject has given informed consent, unless the data controller can show that the data subject in question accessed that information prior to giving consent.

consent, even when the contact details of the data protection officer have not been communicated to the data subject (in the first information layer), pursuant to Article 13(1)(b) or 14(1)(b) GDPR.

### 3.4 Unambiguous indication of wishes

75. The GDPR is clear that consent requires a statement from the data subject or a clear affirmative act, which means that it must always be given through an active motion or declaration. It must be obvious that the data subject has consented to the particular processing.
76. Article 2(h) of Directive 95/46/EC described consent as an “indication of wishes by which the data subject signifies his agreement to personal data relating to him being processed”. Article 4(11) GDPR builds on this definition, by clarifying that valid consent requires an *unambiguous* indication by means of a *statement or by a clear affirmative action*, in line with previous guidance issued by the WP29.
77. A “clear affirmative act” means that the data subject must have taken a deliberate action to consent to the particular processing.<sup>43</sup> Recital 32 sets out additional guidance on this. Consent can be collected through a written or (a recorded) oral statement, including by electronic means.
78. Perhaps the most literal way to fulfil the criterion of a “written statement” is to make sure a data subject writes in a letter or types an email to the controller explaining what exactly he/she agrees to. However, this is often not realistic. Written statements can come in many shapes and sizes that could be compliant with the GDPR.
79. Without prejudice to existing (national) contract law, consent can be obtained through a recorded oral statement, although due note must be taken of the information available to the data subject, prior to the indication of consent. The use of pre-ticked opt-in boxes is invalid under the GDPR. Silence or inactivity on the part of the data subject, as well as merely proceeding with a service cannot be regarded as an active indication of choice.
80. Example 14: When installing software, the application asks the data subject for consent to use non-anonymised crash reports to improve the software. A layered privacy notice providing the necessary information accompanies the request for consent. By actively ticking the optional box stating, “I consent”, the user is able to validly perform a ‘clear affirmative act’ to consent to the processing.
81. A controller must also beware that consent cannot be obtained through the same motion as agreeing to a contract or accepting general terms and conditions of a service. Blanket acceptance of general terms and conditions cannot be seen as a clear affirmative action to consent to the use of personal

---

<sup>43</sup> See Commission Staff Working Paper, Impact Assessment, Annex 2, p. 20 and also pp. 105-106: “As also pointed out in the opinion adopted by WP29 on consent, it seems essential to clarify that valid consent requires the use of mechanisms that leave no doubt of the data subject’s intention to consent, while making clear that – in the context of the on-line environment – the use of default options which the data subject is required to modify in order to reject the processing (‘consent based on silence’) does not in itself constitute unambiguous consent. This would give individuals more control over their own data, whenever processing is based on his/her consent. As regards impact on data controllers, this would not have a major impact as it solely clarifies and better spells out the implications of the current Directive in relation to the conditions for a valid and meaningful consent from the data subject. In particular, to the extent that ‘explicit’ consent would clarify – by replacing “unambiguous” – the modalities and quality of consent and that it is not intended to extend the cases and situations where (explicit) consent should be used as a ground for processing, the impact of this measure on data controllers is not expected to be major.”

data. The GDPR does not allow controllers to offer pre-ticked boxes or opt-out constructions that require an intervention from the data subject to prevent agreement (for example ‘opt-out boxes’).<sup>44</sup>

82. When consent is to be given following a request by electronic means, the request for consent should not be *unnecessarily* disruptive to the use of the service for which the consent is provided.<sup>45</sup> An active affirmative motion by which the data subject indicates consent can be necessary when a less infringing or disturbing modus would result in ambiguity. Thus, it may be necessary that a consent request interrupts the use experience to some extent to make that request effective.
  83. However, within the requirements of the GDPR, controllers have the liberty to develop a consent flow that suits their organisation. In this regard, physical motions can be qualified as a clear affirmative action in compliance with the GDPR.
  84. Controllers should design consent mechanisms in ways that are clear to data subjects. Controllers must avoid ambiguity and must ensure that the action by which consent is given can be distinguished from other actions. Therefore, merely continuing the ordinary use of a website is not conduct from which one can infer an indication of wishes by the data subject to signify his or her agreement to a proposed processing operation.
85. Example 15: Swiping a bar on a screen, waiving in front of a smart camera, turning a smartphone around clockwise, or in a figure eight motion may be options to indicate agreement, as long as clear information is provided, and it is clear that the motion in question signifies agreement to a specific request (e.g. if you swipe this bar to the left, you agree to the use of information X for purpose Y. Repeat the motion to confirm.”). The controller must be able to demonstrate that consent was obtained this way and data subjects must be able to withdraw consent as easily as it was given.
86. Example 16: Based on recital 32, actions such as scrolling or swiping through a webpage or similar user activity will not under any circumstances satisfy the requirement of a clear and affirmative action: such actions may be difficult to distinguish from other activity or interaction by a user and therefore determining that an unambiguous consent has been obtained will also not be possible. Furthermore, in such a case, it will be difficult to provide a way for the user to withdraw consent in a manner that is as easy as granting it.
  87. In the digital context, many services need personal data to function, hence, data subjects receive multiple consent requests that need answers through clicks and swipes every day. This may result in a certain degree of click fatigue: when encountered too many times, the actual warning effect of consent mechanisms is diminishing.
  88. This results in a situation where consent questions are no longer read. This is a particular risk to data subjects, as, typically, consent is asked for actions that are in principle unlawful without their consent. The GDPR places upon controllers the obligation to develop ways to tackle this issue.
  89. An often-mentioned example to do this in the online context is to obtain consent of Internet users via their browser settings. Such settings should be developed in line with the conditions for valid consent

---

<sup>44</sup> See Article 7(2). See also Working Document 02/2013 on obtaining consent for cookies (WP 208), pp. 3-6.

<sup>45</sup> See Recital 32 GDPR.

in the GDPR, as for instance that the consent shall be granular for each of the envisaged purposes and that the information to be provided, should name the controllers.

90. In any event, consent must always be obtained before the controller starts processing personal data for which consent is needed. WP29 has consistently held in its opinions that consent should be given prior to the processing activity.<sup>46</sup> Although the GDPR does not literally prescribe in Article 4(11) that consent must be given prior to the processing activity, this is clearly implied. The heading of Article 6(1) and the wording “has given” in Article 6(1)(a) support this interpretation. It follows logically from Article 6 and Recital 40 that a valid lawful basis must be present before starting a data processing. Therefore, consent should be given prior to the processing activity. In principle, it can be sufficient to ask for a data subject’s consent once. However, controllers do need to obtain a new and specific consent if purposes for data processing change after consent was obtained or if an additional purpose is envisaged.

## 4 OBTAINING EXPLICIT CONSENT

91. Explicit consent is required in certain situations where serious data protection risk emerge, hence, where a high level of individual control over personal data is deemed appropriate. Under the GDPR, explicit consent plays a role in Article 9 on the processing of special categories of data, the provisions on data transfers to third countries or international organisations in the absence of adequate safeguards in Article 49<sup>47</sup>, and in Article 22 on automated individual decision-making, including profiling.<sup>48</sup>
92. The GDPR prescribes that a “statement or clear affirmative action” is a prerequisite for ‘regular’ consent. As the ‘regular’ consent requirement in the GDPR is already raised to a higher standard compared to the consent requirement in Directive 95/46/EC, it needs to be clarified what extra efforts a controller should undertake in order to obtain the *explicit* consent of a data subject in line with the GDPR.
93. The term *explicit* refers to the way consent is expressed by the data subject. It means that the data subject must give an express statement of consent. An obvious way to make sure consent is explicit would be to expressly confirm consent in a written statement. Where appropriate, the controller could

---

<sup>46</sup> WP29 has consistently held this position since Opinion 15/2011 on the definition of consent (WP 187), pp. 30-31.

<sup>47</sup> According to Article 49 (1)(a) GDPR, explicit consent can lift the ban on data transfers to countries without adequate levels of data protection law. Also note Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 (WP 114), p. 11, where WP29 has indicated that consent for data transfers that occur periodically or on an on-going basis is inappropriate.

<sup>48</sup> In Article 22, the GDPR introduces provisions to protect data subjects against decision-making based solely on automated processing, including profiling. Decisions made on this basis are allowed under certain legal conditions. Consent plays a key role in this protection mechanism, as Article 22(2)(c) GDPR makes clear that a controller may proceed with automated decision making, including profiling, that may significantly affect the individual, with the data subject’s explicit consent. WP29 have produced separate guidelines on this issue: WP29 Guidelines on Automated decision-making and Profiling for the purposes of Regulation 2016/679, 3 October 2017 (WP 251).

make sure the written statement is signed by the data subject, in order to remove all possible doubt and potential lack of evidence in the future.<sup>49</sup>

94. However, such a signed statement is not the only way to obtain explicit consent and, it cannot be said that the GDPR prescribes written and signed statements in all circumstances that require valid explicit consent. For example, in the digital or online context, a data subject may be able to issue the required statement by filling in an electronic form, by sending an email, by uploading a scanned document carrying the signature of the data subject, or by using an electronic signature. In theory, the use of oral statements can also be sufficiently express to obtain valid explicit consent, however, it may be difficult to prove for the controller that all conditions for valid explicit consent were met when the statement was recorded.
95. An organisation may also obtain explicit consent through a telephone conversation, provided that the information about the choice is fair, intelligible and clear, and it asks for a specific confirmation from the data subject (e.g. pressing a button or providing oral confirmation).
96. Example 17: A data controller may also obtain explicit consent from a visitor to its website by offering an explicit consent screen that contains Yes and No check boxes, provided that the text clearly indicates the consent, for instance “I, hereby, consent to the processing of my data”, and not for instance, “It is clear to me that my data will be processed”. It goes without saying that the conditions for informed consent as well as the other conditions for obtaining valid consent should be met.
97. Example 18: A clinic for cosmetic surgery seeks explicit consent from a patient to transfer his medical record to an expert whose second opinion is asked on the condition of the patient. The medical record is a digital file. Given the specific nature of the information concerned, the clinic asks for an electronic signature of the data subject to obtain valid explicit consent and to be able to demonstrate that explicit consent was obtained.<sup>50</sup>
98. Two stage verification of consent can also be a way to make sure explicit consent is valid. For example, a data subject receives an email notifying them of the controller’s intent to process a record containing medical data. The controller explains in the email that he asks for consent for the use of a specific set of information for a specific purpose. If the data subjects agrees to the use of this data, the controller asks him or her for an email reply containing the statement ‘I agree’. After the reply is sent, the data subject receives a verification link that must be clicked, or an SMS message with a verification code, to confirm agreement.
99. Article 9(2) does not recognize “necessary for the performance of a contract” as an exception to the general prohibition to process special categories of data. Therefore, controllers and Member States that deal with this situation should explore the specific exceptions in Article 9(2) subparagraphs (b) to (j). Should none of the exceptions (b) to (j) apply, obtaining explicit consent in accordance with the conditions for valid consent in the GDPR remains the only possible lawful exception to process such data.

---

<sup>49</sup> See also WP29 Opinion 15/2011, on the definition of consent (WP 187), p. 25.

<sup>50</sup> This example is without prejudice to EU Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.

100. Example 19: An airline company, Holiday Airways, offers an assisted travelling service for passengers that cannot travel unassisted, for example due to a disability. A customer books a flight from Amsterdam to Budapest and requests travel assistance to be able to board the plane. Holiday Airways requires her to provide information on her health condition to be able to arrange the appropriate services for her (hence, there are many possibilities e.g. wheelchair on the arrival gate, or an assistant travelling with her from A to B.) Holiday Airways asks for explicit consent to process the health data of this customer for the purpose of arranging the requested travel assistance. -The data processed on the basis of consent should be necessary for the requested service. Moreover, flights to Budapest remain available without travel assistance. Please note that since that data are necessary for the provision of the requested service, Article 7 (4) does not apply.
101. Example 20: A successful company is specialised in providing custom-made ski- and snowboard goggles, and other types of customised eyewear for outdoors sports. The idea is that people could wear these without their own glasses on. The company receives orders at a central point and delivers products from a single location all across the EU.
102. In order to be able to provide its customised products to customers who are short-sighted, this controller requests consent for the use of information on customers' eye condition. Customers provide the necessary health data, such as their prescription data online when they place their order. Without this, it is not possible to provide the requested customized eyewear. The company also offers series of goggles with standardized correctional values. Customers that do not wish to share health data could opt for the standard versions. Therefore, an explicit consent under Article 9 is required and consent can be considered to be freely given.

## 5 ADDITIONAL CONDITIONS FOR OBTAINING VALID CONSENT

103. The GDPR introduces requirements for controllers to make additional arrangements to ensure they obtain, and maintain and are able to demonstrate, valid consent. Article 7 of the GDPR sets out these additional conditions for valid consent, with specific provisions on keeping records of consent and the right to easily withdraw consent. Article 7 also applies to consent referred to in other articles of GDPR, e.g. Articles 8 and 9. Guidance on the additional requirement to demonstrate valid consent and on withdrawal of consent is provided below.
- 5.1 Demonstrate consent**
104. In Article 7(1), the GDPR clearly outlines the explicit obligation of the controller to demonstrate a data subject's consent. The burden of proof will be on the controller, according to Article 7(1).
105. Recital 42 states: "*Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation.*"
106. Controllers are free to develop methods to comply with this provision in a way that is fitting in their daily operations. At the same time, the duty to demonstrate that valid consent has been obtained by a controller, should not in itself lead to excessive amounts of additional data processing. This means that controllers should have enough data to show a link to the processing (to show consent was obtained) but they shouldn't be collecting any more information than necessary.
107. It is up to the controller to prove that valid consent was obtained from the data subject. The GDPR does not prescribe exactly how this must be done. However, the controller must be able to prove that a data subject in a given case has consented. As long as a data processing activity in question lasts, the

obligation to demonstrate consent exists. After the processing activity ends, proof of consent should be kept no longer than strictly necessary for compliance with a legal obligation or for the establishment, exercise or defence of legal claims, in accordance with Article 17(3)(b) and (e).

108. For instance, the controller may keep a record of consent statements received, so he can show how consent was obtained, when consent was obtained and the information provided to the data subject at the time shall be demonstrable. The controller shall also be able to show that the data subject was informed and the controller's workflow met all relevant criteria for a valid consent. The rationale behind this obligation in the GDPR is that controllers must be accountable with regard to obtaining valid consent from data subjects and the consent mechanisms they have put in place. For example, in an online context, a controller could retain information on the session in which consent was expressed, together with documentation of the consent workflow at the time of the session, and a copy of the information that was presented to the data subject at that time. It would not be sufficient to merely refer to a correct configuration of the respective website.

109. Example 21: A hospital sets up a scientific research programme, called project X, for which dental records of real patients are necessary. Participants are recruited via telephone calls to patients that voluntarily agreed to be on a list of candidates that may be approached for this purpose. The controller seeks explicit consent from the data subjects for the use of their dental record. Consent is obtained during a phone call by recording an oral statement of the data subject in which the data subject confirms that they agree to the use of their data for the purposes of project X.

110. There is no specific time limit in the GDPR for how long consent will last. How long consent lasts will depend on the context, the scope of the original consent and the expectations of the data subject. If the processing operations change or evolve considerably then the original consent is no longer valid. If this is the case, then new consent needs to be obtained.
111. The EDPB recommends as a best practice that consent should be refreshed at appropriate intervals. Providing all the information again helps to ensure the data subject remains well informed about how their data is being used and how to exercise their rights.<sup>51</sup>

## 5.2 Withdrawal of consent

112. Withdrawal of consent is given a prominent place in the GDPR. The provisions and recitals on withdrawal of consent in the GDPR can be regarded as codification of the existing interpretation of this matter in WP29 Opinions.<sup>52</sup>
113. Article 7(3) of the GDPR prescribes that the controller must ensure that consent can be withdrawn by the data subject as easy as giving consent and at any given time. The GDPR does not say that giving and withdrawing consent must always be done through the same action.
114. However, when consent is obtained via electronic means through only one mouse-click, swipe, or keystroke, data subjects must, in practice, be able to withdraw that consent equally as easily. Where

---

<sup>51</sup> See Article 29 Working Party guidelines on transparency under Regulation 2016/679 WP260 rev.01 - endorsed by the EDPB.

<sup>52</sup> WP29 has discussed this subject in their Opinion on consent (see Opinion 15/2011 on the definition of consent (WP 187), pp. 9, 13, 20, 27 and 32-33) and, inter alia, their Opinion on the use of location data. (see Opinion 5/2005 on the use of location data with a view to providing value-added services (WP 115), p. 7).

consent is obtained through use of a service-specific user interface (for example, via a website, an app, a log-on account, the interface of an IoT device or by e-mail), there is no doubt a data subject must be able to withdraw consent via the same electronic interface, as switching to another interface for the sole reason of withdrawing consent would require undue effort. Furthermore, the data subject should be able to withdraw his/her consent without detriment. This means, *inter alia*, that a controller must make withdrawal of consent possible free of charge or without lowering service levels.<sup>53</sup>

115. **Example 22:** A music festival sells tickets through an online ticket agent. With each online ticket sale, consent is requested in order to use contact details for marketing purposes. To indicate consent for this purpose, customers can select either No or Yes. The controller informs customers that they have the possibility to withdraw consent. To do this, they could contact a call centre on business days between 8am and 5pm, free of charge. The controller in this example does not comply with article 7(3) of the GDPR. Withdrawing consent in this case requires a telephone call during business hours, this is more burdensome than the one mouse-click needed for giving consent through the online ticket vendor, which is open 24/7.
116. The requirement of an easy withdrawal is described as a necessary aspect of valid consent in the GDPR. If the withdrawal right does not meet the GDPR requirements, then the consent mechanism of the controller does not comply with the GDPR. As mentioned in section 3.1 on the condition of *informed* consent, the controller must inform the data subject of the right to withdraw consent prior to actually giving consent, pursuant to Article 7(3) of the GDPR. Additionally, the controller must as part of the transparency obligation inform the data subjects on how to exercise their rights.<sup>54</sup>
117. As a general rule, if consent is withdrawn, all data processing operations that were based on consent and took place before the withdrawal of consent - and in accordance with the GDPR - remain lawful, however, the controller must stop the processing actions concerned. If there is no other lawful basis justifying the processing (e.g. further storage) of the data, they should be deleted by the controller.<sup>55</sup>
118. As mentioned earlier in these guidelines, it is very important that controllers assess the purposes for which data is actually processed and the lawful grounds on which it is based prior to collecting the data. Often companies need personal data for several purposes, and the processing is based on more than one lawful basis, e.g. customer data may be based on contract and consent. Hence, a withdrawal of consent does not mean a controller must erase data that are processed for a purpose that is based on the performance of the contract with the data subject. Controllers should therefore be clear from the outset about which purpose applies to each element of data and which lawful basis is being relied upon.

---

<sup>53</sup> See also opinion WP29 Opinion 4/2010 on the European code of conduct of FEDMA for the use of personal data in direct marketing (WP 174) and the Opinion on the use of location data with a view to providing value-added services (WP 115).

<sup>54</sup> Recital 39 GDPR, which refers to Articles 13 and 14 of that Regulation, states that "*natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing.*

<sup>55</sup> See Article 17(1)(b) and (3) GDPR.

- 119. Controllers have an obligation to delete data that was processed on the basis of consent once that consent is withdrawn, assuming that there is no other purpose justifying the continued retention.<sup>56</sup> Besides this situation, covered in Article 17 (1)(b), an individual data subject may request erasure of other data concerning him that is processed on another lawful basis, e.g. on the basis of Article 6(1)(b).<sup>57</sup> Controllers are obliged to assess whether continued processing of the data in question is appropriate, even in the absence of an erasure request by the data subject.<sup>58</sup>
- 120. In cases where the data subject withdraws his/her consent and the controller wishes to continue to process the personal data on another lawful basis, they cannot silently migrate from consent (which is withdrawn) to this other lawful basis. Any change in the lawful basis for processing must be notified to a data subject in accordance with the information requirements in Articles 13 and 14 and under the general principle of transparency.

## 6 INTERACTION BETWEEN CONSENT AND OTHER LAWFUL GROUNDS IN ARTICLE 6 GDPR

- 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.<sup>59</sup>
- 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.
- 123. In other words, the controller cannot swap from consent to other lawful bases. For example, it is not allowed to retrospectively utilise the legitimate interest basis in order to justify processing, where problems have been encountered with the validity of consent. Because of the requirement to disclose the lawful basis, which the controller is relying upon at the time of collection of personal data, controllers must have decided in advance of collection what the applicable lawful basis is.

## 7 SPECIFIC AREAS OF CONCERN IN THE GDPR

### 7.1 Children (Article 8)

- 124. Compared to the current directive, the GDPR creates an additional layer of protection where personal data of vulnerable natural persons, especially children, are processed. Article 8 introduces additional obligations to ensure an enhanced level of data protection of children in relation to information society services. The reasons for the enhanced protection are specified in Recital 38: “ [...] they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the

---

<sup>56</sup> In that case, the other purpose justifying the processing must have its own separate legal basis. This does not mean the controller can swap from consent to another lawful basis, see section 6 below.

<sup>57</sup> See Article 17, including exceptions that may apply, and Recital 65 GDPR.

<sup>58</sup> See also Article 5 (1)(e) GDPR.

<sup>59</sup> Pursuant to Articles 13 (1)(c) and/or 14(1)(c), the controller must inform the data subject thereof.

*processing of personal data [...]” Recital 38 also states that “Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child.”* The words ‘in particular’ indicate that the specific protection is not confined to marketing or profiling but includes the wider ‘collection of personal data with regard to children’.

125. Article 8(1) states that where consent applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.<sup>60</sup> Regarding the age limit of valid consent the GDPR provides flexibility, Member States can provide by law a lower age, but this age cannot be below 13 years.
126. As mentioned in section 3.1. on informed consent, the information shall be understandable to the audience addressed by the controller, paying particular attention to the position of children. In order to obtain “informed consent” from a child, the controller must explain in language that is clear and plain for children how it intends to process the data it collects.<sup>61</sup> If it is the parent that is supposed to consent, then a set of information may be required that allows adults to make an informed decision.
127. It is clear from the foregoing that Article 8 shall only apply when the following conditions are met:
  - ) The processing is related to the offer of information society services directly to a child.<sup>62, 63</sup>
  - ) The processing is based on consent.

#### 7.1.1 Information society service

128. To determine the scope of the term ‘information society service’ in the GDPR, reference is made in Article 4(25) GDPR to Directive 2015/1535.

---

<sup>60</sup> Without prejudice to the possibility of Member State law to derogate from the age limit, see Article 8(1).

<sup>61</sup> Recital 58 GDPR re-affirms this obligation, in stating that, where appropriate, a controller should make sure the information provided is understandable for children.

<sup>62</sup> According to Article 4(25) GDPR an information society service means a service as defined in point (b) of Article 1(1) of Directive 2015/1535: “(b) ‘service’ means any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. For the purposes of this definition: (i) ‘at a distance’ means that the service is provided without the parties being simultaneously present; (ii) ‘by electronic means’ means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means; (iii) ‘at the individual request of a recipient of services’ means that the service is provided through the transmission of data on individual request.” An indicative list of services not covered by this definition is set out in Annex I of the said Directive. See also Recital 18 of Directive 2000/31.

<sup>63</sup> According to the UN Convention on the Protection of the Child, Article 1, “[...] a child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier,” see United Nations, General Assembly Resolution 44/25 of 20 November 1989 (Convention on the Rights of the Child).

129. While assessing the scope of this definition, the EDPB also refers to case law of the ECJ.<sup>64</sup> The ECJ held that *information society services* cover contracts and other services that are concluded or transmitted on-line. Where a service has two economically independent components, one being the online component, such as the offer and the acceptance of an offer in the context of the conclusion of a contract or the information relating to products or services, including marketing activities, this component is defined as an information society service, the other component being the physical delivery or distribution of goods is not covered by the notion of an information society service. The online delivery of a service would fall within the scope of the term *information society service* in Article 8 GDPR.

#### 7.1.2 Offered directly to a child

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

#### 7.1.3 Age

131. The GDPR specifies that “*Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.*” The controller must be aware of those different national laws, by taking into account the public targeted by its services. In particular, it should be noted that a controller providing a cross-border service cannot always rely on complying with only the law of the Member State in which it has its main establishment but may need to comply with the respective national laws of each Member State in which it offers the information society service(s). This depends on whether a Member State chooses to use the place of main establishment of the controller as a point of reference in its national law, or the residence of the data subject. First of all the Member States shall consider the best interests of the child during making their choice. The Working Group encourages the Member States to search for a harmonized solution in this matter.
132. When providing information society services to children on the basis of consent, controllers will be expected to make reasonable efforts to verify that the user is over the age of digital consent, and these measures should be proportionate to the nature and risks of the processing activities.
133. If the users state that they are over the age of digital consent then the controller can carry out appropriate checks to verify that this statement is true. Although the need to undertake reasonable efforts to verify age is not explicit in the GDPR it is implicitly required, for if a child gives consent while not old enough to provide valid consent on their own behalf, then this will render the processing of data unlawful.
134. If the user states that he/she is below the age of digital consent then the controller can accept this statement without further checks, but will need to go on to obtain parental authorisation and verify that the person providing that consent is a holder of parental responsibility.

---

<sup>64</sup> See European Court of Justice, 2 December 2010 Case C-108/09, (*Ker-Optika*), paragraphs 22 and 28. In relation to ‘composite services’, the EDPB also refers to Case C-434/15 (*Asociacion Profesional Elite Taxi v Uber Systems Spain SL*), para 40, which states that an information society service forming an integral part of an overall service whose main component is not an information society service (in this case a transport service), must not be qualified as ‘an information society service’.

135. Age verification should not lead to excessive data processing. The mechanism chosen to verify the age of a data subject should involve an assessment of the risk of the proposed processing. In some low-risk situations, it may be appropriate to require a new subscriber to a service to disclose their year of birth or to fill out a form stating they are (not) a minor.<sup>65</sup> If doubts arise, the controller should review their age verification mechanisms in a given case and consider whether alternative checks are required.<sup>66</sup>

#### 7.1.4 Children's consent and parental responsibility

136. Regarding the authorisation of a holder of parental responsibility, the GDPR does not specify practical ways to gather the parent's consent or to establish that someone is entitled to perform this action.<sup>67</sup> Therefore, the EDPB recommends the adoption of a proportionate approach, in line with Article 8(2) GDPR and Article 5(1)(c) GDPR (data minimisation). A proportionate approach may be to focus on obtaining a limited amount of information, such as contact details of a parent or guardian.
137. What is reasonable, both in terms of verifying that a user is old enough to provide their own consent, and in terms of verifying that a person providing consent on behalf of a child is a holder of parental responsibility, may depend upon the risks inherent in the processing as well as the available technology. In low-risk cases, verification of parental responsibility via email may be sufficient. Conversely, in high-risk cases, it may be appropriate to ask for more proof, so that the controller is able to verify and retain the information pursuant to Article 7(1) GDPR.<sup>68</sup> Trusted third party verification services may offer solutions, which minimise the amount of personal data the controller has to process itself.

138. Example 23: An online gaming platform wants to make sure underage customers only subscribe to its services with the consent of their parents or guardians. The controller follows these steps:
139. Step 1: ask the user to state whether they are under or over the age of 16 (or alternative age of digital consent) If the user states that they are under the age of digital consent:
140. Step 2: service informs the child that a parent or guardian needs to consent or authorise the processing before the service is provided to the child. The user is requested to disclose the email address of a parent or guardian.
141. Step 3: service contacts the parent or guardian and obtains their consent via email for processing and take reasonable steps to confirm that the adult has parental responsibility.
142. Step 4: in case of complaints, the platform takes additional steps to verify the age of the subscriber.

---

<sup>65</sup> Although this may not be a watertight solution in all cases, it is an example to deal with this provision

<sup>66</sup> See WP29 Opinion 5/2009 on social networking services (WP 163).

<sup>67</sup> WP 29 notes that it not always the case that the holder of parental responsibility is the natural parent of the child and that parental responsibility can be held by multiple parties which may include legal as well as natural persons.

<sup>68</sup> For example, a parent or guardian could be asked to make a payment of €0,01 to the controller via a bank transaction, including a brief confirmation in the description line of the transaction that the bank account holder is a holder of parental responsibility over the user. Where appropriate, an alternative method of verification should be provided to prevent undue discriminatory treatment of persons that do not have a bank account.

143. If the platform has met the other consent requirements, the platform can comply with the additional criteria of Article 8 GDPR by following these steps.

144. The example shows that the controller can put itself in a position to show that reasonable efforts have been made to ensure that valid consent has been obtained, in relation to the services provided to a child. Article 8(2) particularly adds that "*The controller shall make reasonable efforts to verify that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.*"
145. It is up to the controller to determine what measures are appropriate in a specific case. As a general rule, controllers should avoid verification solutions which themselves involve excessive collection of personal data.
146. The EDPB acknowledges that there may be cases where verification is challenging (for example where children providing their own consent have not yet established an 'identity footprint', or where parental responsibility is not easily checked. This can be taken into account when deciding what efforts are reasonable, but controllers will also be expected to keep their processes and the available technology under constant review.
147. With regard to the data subject's autonomy to consent to the processing of their personal data and have full control over the processing, consent by a holder of parental responsibility or authorized by a holder of parental responsibility for the processing of personal data of children can be confirmed, modified or withdrawn, once the data subject reaches the age of digital consent.
148. In practice, this means that if the child does not take any action, consent given by a holder of parental responsibility or authorized by a holder of parental responsibility for the processing of personal data given prior to the age of digital consent, will remain a valid ground for processing.
149. After reaching the age of digital consent, the child will have the possibility to withdraw the consent himself, in line with Article 7(3). In accordance with the principles of fairness and accountability, the controller must inform the child about this possibility.<sup>69</sup>
150. It is important to point out that in accordance with Recital 38, consent by a parent or guardian is not required in the context of preventive or counselling services offered directly to a child. For example the provision of child protection services offered online to a child by means of an online chat service do not require prior parental authorisation.
151. Finally, the GDPR states that the rules concerning parental authorization requirements vis-à-vis minors shall not interfere with "the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child". Therefore, the requirements for valid consent for the use of data about children are part of a legal framework that must be regarded as separate from national contract law. Therefore, this guidance paper does not deal with the question whether it is lawful for a minor to conclude online contracts. Both legal regimes may apply simultaneously, and, the scope of the GDPR does not include harmonization of national provisions of contract law.

---

<sup>69</sup> Also, data subjects should be aware of the right to be forgotten as laid down in Article 17, which is in particular relevant for consent given when the data subject was still a child, see recital 63.

152.

## 7.2 Scientific research

153. The definition of scientific research purposes has substantial ramifications for the range of data processing activities a controller may undertake. The term '*scientific research*' is not defined in the GDPR. Recital 159 states “(...) *For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner.* (...)”, however the EDPB considers 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.
154. When consent is the legal basis for conducting research in accordance with the GDPR, this consent for the use of personal data should be distinguished from other consent requirements that serve as an ethical standard or procedural obligation. An example of such a procedural obligation, where the processing is based not on consent but on another legal basis, is to be found in the Clinical Trials Regulation. In the context of data protection law, the latter form of consent could be considered as an additional safeguard.<sup>70</sup> At the same time, the GDPR does not restrict the application of Article 6 to consent alone, with regard to processing data for research purposes. As long as appropriate safeguards are in place, such as the requirements under Article 89(1), and the processing is fair, lawful, transparent and accords with data minimisation standards and individual rights, other lawful bases such as Article 6(1)(e) or (f) may be available.<sup>71</sup> This also applies to special categories of data pursuant to the derogation of Article 9(2)(j).<sup>72</sup>
155. Recital 33 seems to bring some flexibility to the degree of specification and granularity of consent in the context of scientific research. Recital 33 states: “*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.*”
156. First, it should be noted that Recital 33 does not disapply the obligations with regard to the requirement of specific consent. This means that, in principle, scientific research projects can only include personal data on the basis of consent if they have a well-described purpose. For the cases where purposes for data processing within a scientific research project cannot be specified at the outset, Recital 33 allows as an exception that the purpose may be described at a more general level.
157. Considering the strict conditions stated by Article 9 GDPR regarding the processing of special categories of data, the EDPB notes that when special categories of data are processed on the basis of explicit

---

<sup>70</sup> See also Recital 161 of the GDPR.

<sup>71</sup> Article 6(1)(c) may also be applicable for parts of the processing operations specifically required by law, such as gathering reliable and robust data following the protocol as approved by the Member State under the Clinical Trial Regulation.

<sup>72</sup> Specific testing of medicinal products may take place on the basis of an EU or national law pursuant to Article 9(2)(i).

consent, applying the flexible approach of Recital 33 will be subject to a stricter interpretation and requires a high degree of scrutiny.

158. When regarded as a whole, the GDPR cannot be interpreted to allow for a controller to navigate around the key principle of specifying purposes for which consent of the data subject is asked.
159. When research purposes cannot be fully specified, a controller must seek other ways to ensure the essence of the consent requirements are served best, for example, to allow data subjects to consent for a research purpose in more general terms and for specific stages of a research project that are already known to take place at the outset. As the research advances, consent for subsequent steps in the project can be obtained before that next stage begins. Yet, such a consent should still be in line with the applicable ethical standards for scientific research.
160. Moreover, the controller may apply further safeguards in such cases. Article 89(1), for example, highlights the need for safeguards in data processing activities for scientific or historical or statistical purposes. These purposes "*shall be subject to appropriate safeguards, in accordance with this regulation, for the rights and freedoms of data subject.*" Data minimization, anonymisation and data security are mentioned as possible safeguards.<sup>73</sup> Anonymisation is the preferred solution as soon as the purpose of the research can be achieved without the processing of personal data.
161. Transparency is an additional safeguard when the circumstances of the research do not allow for a specific consent. A lack of purpose specification may be offset by information on the development of the purpose being provided regularly by controllers as the research project progresses so that, over time, the consent will be as specific as possible. When doing so, the data subject has at least a basic understanding of the state of play, allowing him/her to assess whether or not to use, for example, the right to withdraw consent pursuant to Article 7(3).<sup>74</sup>
162. Also, having a comprehensive research plan available for data subjects to take note of, before they consent could help to compensate a lack of purpose specification.<sup>75</sup> This research plan should specify the research questions and working methods envisaged as clearly as possible. The research plan could also contribute to compliance with Article 7(1), as controllers need to show what information was

---

<sup>73</sup> See for example Recital 156. The processing of personal data for scientific purposes should also comply with other relevant legislation such as on clinical trials, see Recital 156, mentioning 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. See also WP29 Opinion 15/2011 on the definition of consent (WP 187), p. 7: "*Moreover, obtaining consent does not negate the controller's obligations under Article 6 with regard to fairness, necessity and proportionality, as well as data quality. For instance, even if the processing of personal data is based on the consent of the user, this would not legitimise the collection of data which is excessive in relation to a particular purpose.*" [...] *As a principle, consent should not be seen as an exemption from the other data protection principles, but as a safeguard. It is primarily a ground for lawfulness, and it does not waive the application of other principles.*"

<sup>74</sup> Other transparency measures may also be relevant. When controllers engage in data processing for scientific purposes, while full information cannot be provided at the outset, they could designate a specific contact person for data subjects to address with questions.

<sup>75</sup> Such a possibility can be found in Article 14(1) of the current Personal Data Act of Finland (*Henkilötietolaki*, 523/1999).

available to data subjects at the time of consent in order to be able to demonstrate that consent is valid.

163. It is important to recall that where consent is being used as the lawful basis for processing there must be a possibility for a data subject to withdraw that consent. The EDPB notes that withdrawal of consent could undermine types scientific research that require data that can be linked to individuals, however the GDPR is clear that consent can be withdrawn and controllers must act upon this – there is no exemption to this requirement for scientific research. If a controller receives a withdrawal request, it must in principle delete the personal data straight away if it wishes to continue to use the data for the purposes of the research.<sup>76</sup>

### 7.3 Data subject's rights

164. If a data processing activity is based on a data subject's consent, this will affect that individual's rights. Data subjects may have the right to data portability (Article 20) when processing is based on consent. At the same time, the right to object (Article 21) does not apply when processing is based on consent, although the right to withdraw consent at any time may provide a similar outcome.
165. Articles 16 to 20 of the GDPR indicate that (when data processing is based on consent), data subjects have the right to erasure when consent has been withdrawn and the rights to restriction, rectification and access.<sup>77</sup>

## 8 CONSENT OBTAINED UNDER DIRECTIVE 95/46/EC

166. Controllers that currently process data on the basis of consent in compliance with national data protection law are not automatically required to completely refresh all existing consent relations with data subjects in preparation for the GDPR. Consent, which has been obtained, to date continues to be valid in so far as it is in line with the conditions laid down in the GDPR.
167. It is important for controllers to review current work processes and records in detail, before 25 May 2018, to be sure existing consents meet the GDPR standard (see Recital 171 of the GDPR<sup>78</sup>). In practice, the GDPR raises the bar with regard to implementing consent mechanisms and introduces several new

---

<sup>76</sup> See also WP29 Opinion 05/2014 on "Anonymisation Techniques" (WP216).

<sup>77</sup> In cases where certain data processing activities are restricted in accordance with Article 18, GDPR, consent of the data subject may be needed to lift restrictions.

<sup>78</sup> Recital 171 GDPR states: "*Directive 95/46/EC should be repealed by this Regulation. Processing already under way on the date of application of this Regulation should be brought into conformity with this Regulation within the period of two years after which this Regulation enters into force. Where processing is based on consent pursuant to Directive 95/46/EC, it is not necessary for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of this Regulation, so as to allow the controller to continue such processing after the date of application of this Regulation. Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC remain in force until amended, replaced or repealed.*"

requirements that require controllers to alter consent mechanisms, rather than rewriting privacy policies alone.<sup>79</sup>

168. For example, as the GDPR requires that a controller must be able to demonstrate that valid consent was obtained, all presumed consents of which no references are kept will automatically be below the consent standard of the GDPR and will need to be renewed. Likewise as the GDPR requires a “statement or a clear affirmative action”, all presumed consents that were based on a more implied form of action by the data subject (e.g. a pre-ticked opt-in box) will also not be apt to the GDPR standard of consent.
169. Furthermore, to be able to demonstrate that consent was obtained or to allow for more granular indications of the data subject’s wishes, operations and IT systems may need revision. Also, mechanisms for data subjects to withdraw their consent easily must be available and information about how to withdraw consent must be provided. If existing procedures for obtaining and managing consent do not meet the GDPR’s standards, controllers will need to obtain fresh GDPR compliant consent.
170. On the other hand, as not all elements named in Articles 13 and 14 must always be present as a condition for informed consent, the extended information obligations under the GDPR do not necessarily oppose the continuity of consent, which has been granted before the GDPR enters into force (see page 15 above). Under Directive 95/46/EC, there was no requirement to inform data subjects of the basis upon which the processing was being conducted.
171. If a controller finds that the consent previously obtained under the old legislation will not meet the standard of GDPR consent, then controllers must undertake action to comply with these standards, for example by refreshing consent in a GDPR-compliant way. Under the GDPR, it is not possible to swap between one lawful basis and another. If a controller is unable to renew consent in a compliant way and is also unable –as a one off situation- to make the transition to GDPR compliance by basing data processing on a different lawful basis while ensuring that continued processing is fair and accounted for, the processing activities must be stopped. In any event, the controller needs to observe the principles of lawful, fair and transparent processing.

---

<sup>79</sup> As indicated in the introduction, the GDPR provides further clarification and specification of the requirements for obtaining and demonstrating valid consent. Many of the new requirements build upon Opinion 15/2011 on consent.

# Guidelines



**Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR**

**Version 2.0**

**Adopted on 15 December 2020**

## Version history

Version 2.0	15.12.2020	Adoption of the Guidelines after public consultation
Version 1.0	17.07.2020	Adoption of the Guidelines for publication consultation

## Table of contents

1. Introduction.....	5
1.1 Definitions .....	6
1.2 Services under the PSD2.....	7
2 Lawful grounds and further processing under the PSD2 .....	9
2.1 Lawful grounds for processing .....	9
2.2 Article 6(1)(b) of the GDPR (processing is necessary for the performance of a contract).....	9
2.3 Fraud prevention.....	11
2.4 Further processing (AISP and PISP) .....	11
2.5 Lawful ground for granting access to the Account (ASPSPs).....	12
3 Explicit Consent .....	13
3.1 Consent under the GDPR.....	13
3.2 Consent under the PSD2 .....	13
3.2.1 Explicit consent under Article 94 (2) PSD2 .....	14
3.3 Conclusion .....	15
4 The processing of silent party data .....	16
4.1 Silent party data .....	16
4.2 The legitimate interest of the controller.....	16
4.3 Further processing of personal data of the silent party.....	16
5 The processing of special categories of personal data under the PSD2 .....	18
5.1 Special categories of personal data.....	18
5.2 Possible derogations .....	19
5.3 Substantial public interest.....	19
5.4 Explicit consent.....	19
5.5 No suitable derogation.....	20
6 Data minimisation, security, transparency, accountability and profiling .....	21
6.1 Data minimisation and data protection by design and default .....	21
6.2 Data minimisation measures.....	21
6.3 Security.....	22
6.4 Transparency and accountability .....	23
6.5 Profiling .....	25

## The European Data Protection Board

Having regard to Article 70 (1) (e) of 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<sup>1</sup>,

Having regard to Article 12 and Article 22 of its Rules of Procedure,

Whereas:

(1) The General Data Protection Regulation provides for a consistent set of rules for the processing of personal data throughout the EU.

(2) The second Payment Services Directive (Directive 2015/2366/EU of the European Parliament and of the Council of 23 December 2015, hereinafter "PSD2") repeals Directive 2007/64/EC and provides new rules to ensure legal certainty for consumers, merchants and companies within the payment chain and modernizing the legal framework for the market for payment services<sup>2</sup>. Member States had to transpose the PSD2 into their national law before the 13 January 2018.

(3) An important feature of the PSD2 is the introduction of a legal framework for new payment initiation services and account information services. The PSD2 allows these new payment service providers to obtain access to payment accounts of data subjects for the purposes of providing the said services.

(4) With regard to data protection, in accordance with Article 94 (1) of the PSD2, any processing of personal data, including the provision of information about the processing, for the purposes of the PSD2, shall be carried out in accordance with the GDPR<sup>3</sup> and with Regulation (EU) No 2018/1725.

(5) Recital 89 of the PSD2 states that where personal data is processed for the purposes of the PSD2, the precise purpose of the processing should be specified, the applicable legal basis should be named, the relevant security requirements laid down in the GDPR must be implemented, and the principles of necessity, proportionality, purpose limitation and proportionate data retention periods respected. Also, data protection by design and data protection by default should be embedded in all data processing systems developed and used within the framework of the PSD2<sup>4</sup>.

(6) Recital 93 of the PSD2 states that the payment initiation service providers and the account information service providers on the one hand and the account servicing payment service provider on the other, should observe the necessary data protection and security requirements established by, or referred to in, this Directive or included in the regulatory technical standards.

---

<sup>1</sup> References to "Member States" made throughout this document should be understood as references to "EEA Member States".

<sup>2</sup> Recital 6 PSD2

<sup>3</sup> As PSD2 predates the GDPR, it still refers to Directive 95/46. Article 94 GDPR states that references to the repealed Directive 95/46 shall be construed as references to the GDPR.

<sup>4</sup> Recital 89, PSD2

## HAS ADOPTED THE FOLLOWING GUIDELINES

### 1. INTRODUCTION

1. The second Payment Services Directive (hereinafter “PSD2”) has introduced a number of novelties in the payment services field. While it creates new opportunities for consumers and enhances transparency in such field, the application of the PSD2 raises certain questions and concerns in respect of the need that the data subjects remain in full control of their personal data. The General Data Protection Regulation (hereinafter “GDPR”) applies to the processing of personal data including processing activities carried out in the context of payment services as defined by the PSD2<sup>5</sup>. Thus, controllers acting in the field covered by the PSD2 must always ensure compliance with the requirements of the GDPR, including the principles of data protection set out in Article 5 of the GDPR, as well as the relevant provisions of the ePrivacy Directive<sup>6</sup>. While the PSD2<sup>7</sup> and the Regulatory Technical Standards for strong customer authentication and common and secure open standards of communication (hereinafter “RTS”<sup>8</sup>) contain certain provisions relating to data protection and security, uncertainty has arisen about the interpretation of these provisions as well as the interplay between the general data protection framework and the PSD2.
2. On July 5 2018, the EDPB issued a letter regarding the PSD2, in which the EDPB provided clarifications on questions concerning the protection of personal data in relation to the PSD2, in particular on the processing of personal data of non-contracting parties (so called ‘silent party data’) by account information service providers (hereinafter “AISPs”) and payment initiation service providers (hereinafter “PISPs”), the procedures with regard to giving and withdrawing consent, the RTS and the cooperation between account servicing payment services providers (hereinafter “ASPSPs”) in relation to security measures. Whereas the preparatory work of these guidelines involved the collection of inputs from stakeholders, both in writing and at a stakeholder event, in order to identify the most pressing challenges.
3. These guidelines aim to provide further guidance on data protection aspects in the context of the PSD2, in particular on the relationship between relevant provisions on the GDPR and the PSD2. The main focus of these guidelines is on the processing of personal data by AISPs and PISPs. As such, this document addresses conditions for granting access to payment account information by ASPSPs and for the processing of personal data by PISPs and AISPs, including the requirements and safeguards in relation to the processing of personal data by PISPs and AISPs for purposes other than the initial purposes for which the data have been collected, especially when they have been collected in the context of the provision of an account information service<sup>9</sup>. This document also

---

<sup>5</sup> Art. 1 (1) GDPR

<sup>6</sup> Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications); OJ L 201, 31/07/2002 P. 0037 - 0047

<sup>7</sup> Art. 94 PSD etc.

<sup>8</sup> Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (Text with EEA relevance.); C/2017/7782; OJ L 69, 13.3.2018, p. 23–43; available at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0389&from=EN>

<sup>9</sup> An account information service is an online service to provide consolidated information on one or more payment accounts held by the payment service user either with another payment service provider or with more than one payment service provider.

addresses different notions of explicit consent under the PSD2 and the GDPR, the processing of ‘silent party data’, the processing of special categories of personal data by PISPs and AISPs, the application of the main data protection principles set forth by the GDPR, including data minimisation, transparency, accountability and security measures. The PSD2 involves cross-functional responsibilities in the fields of, inter alia, consumer protection and competition law. Considerations regarding these fields of law are beyond the scope of these guidelines.

4. To facilitate the reading of the guidelines the main definitions used in this document are provided below.

### **1.1 Definitions**

‘*Account Information Service Provider*’ (‘AISP’) refers to the provider of an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider;

‘*Account Servicing Payment Service Provider*’ (‘ASPSP’) refers to a payment service provider providing and maintaining a payment account for a payer;

‘*Data minimisation*’ is a principle of data protection, according to which personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

‘*Payer*’ refers to a natural or legal person who holds a payment account and allows a payment order from that payment account, or, where there is no payment account, a natural or legal person who gives a payment order;

‘*Payee*’ refers to a natural or legal person who is the intended recipient of funds, which have been the subject of a payment transaction;

‘*Payment account*’ means an account held in the name of one or more payment service users, which is used for the execution of payment transactions;

‘*Payment Initiation Service Provider*’ (‘PISP’) refers to the provider of a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider;

‘*Payment service provider*’ refers to a means a body referred to in Article 1(1) of the PSD2<sup>10</sup> or a natural or legal person benefiting from an exemption pursuant to Article 32 or 33 of the PSD2;

---

<sup>10</sup> Art. 1 (1) PSD2 states that the PSD2 establishes the rules in accordance with which Member States shall distinguish between the following categories of *payment service provider*:

- (a) credit institutions as defined in point (1) of Art. 4(1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council (1), including branches thereof within the meaning of point (17) Art. 4(1) of that Regulation where such branches are located in the Union, whether the head offices of those branches are located within the Union or, in accordance with Art. 47 of Directive 2013/36/EU and with national law, outside the Union;
- (b) electronic money institutions within the meaning of point (1) of Art. 2 of Directive 2009/110/EC, including, in accordance with Art. 8 of that Directive and with national law, branches thereof, where such branches are located within the Union and their head offices are located outside the Union, in as far as the payment services provided by those branches are linked to the issuance of electronic money;
- (c) post office giro institutions which are entitled under national law to provide payment services;
- (d) payment institutions;

*'Payment service user' means a natural or legal person making use of a payment service in the capacity of payer, payee, or both;*

*'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*

*'Data protection by design' refers to technical and organizational measures embedded into a product or service, which are designed to implement data-protection principles, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects;*

*'Data protection by default' refers to appropriate technical and organisational measures implemented in a product or service which ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed;*

*'RTS' refers to the Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication;*

*'Third Party Providers' ('TPP') refers to both PISPs and AISPs.*

## 1.2 Services under the PSD2

5. The PSD2 introduces two new kinds of payment service (providers): PISPs and AISPs. Annex 1 of the PSD2 contains the eight payment services that are covered by the PSD2.
6. PISPs provide services to initiate payment orders at the request of the payment service user with respect to a user's payment account held at another payment service provider<sup>11</sup>. A PISP can request an ASPSP (usually a bank) to initiate a transaction on behalf of the payment service user. The (payment service) user can be a natural person (data subject) or a legal person.
7. AISPs provide online services for consolidated information on one or more payment accounts held by the payment service user either with another payment service provider or with more than one payment service provider<sup>12</sup>. According to recital 28 PSD2, the payment service user is able to have an overall view of its financial situation immediately at any given moment.
8. When it comes to account information services, there could be several different types of services offered, with the emphasis on different features and purposes. For example, some providers may offer users services such as budget planning and monitoring spending. The processing of personal data in the context of these services is covered by the PSD2. Services that entail creditworthiness assessments of the payment service user or audit services performed on the basis of the collection of information via an account information service fall outside of the scope of the PSD2 and therefore fall under the GDPR. Furthermore, accounts other than payment accounts (e.g. savings,

---

(e) the ECB and national central banks when not acting in their capacity as monetary authority or other public authorities;

(f) Member States or their regional or local authorities when not acting in their capacity as public authorities.

<sup>11</sup> Art. 4 (15) PSD2.

<sup>12</sup> Art. 4 (16) PSD2

investments) are not covered by the PSD2 either. In any case, the GDPR is the applicable legal framework for the processing of personal data.

**Example 1:**

HappyPayments is a company that offers an online service consisting of the provision of information on one or more payment accounts through a mobile app in order to provide financial oversight (an Account Information Service). With this service the payment service user can see at a glance the balances and recent transactions in two or more payment accounts at different banks. It also offers, when a payment service user chooses to do so, a categorisation of spending and income according to different typologies (salary, leisure, energy, mortgage, etc.), thus helping the payment service user with financial planning. Within this app, HappyPayments also offers a service to initiate payments directly from the users designated payment account(s) (a Payment Initiation Service).

9. In order to provide those services, the PSD2 regulates the legal conditions under which PISPs and AISP can access payment accounts to provide a service to the payment service user.
10. Articles 66 (1) and 67 (1) PSD2 determine that the access and the use of payment and account information services are rights of the payment service user. This means that the payment service user should remain entirely free with regard to the exercise of such right and cannot be forced to make use of this right.
11. Access to payment accounts and the use of payment account information is partly regulated in Articles 66 and 67 PSD2, which contain safeguards regarding the protection of (personal) data. Article 66 (3) (f) PSD2 states that the PISP shall not request from the payment service user any data other than those necessary to provide the payment initiation service, and Article 66 (3) (g) PSD2 provides that PISPs shall not use, access or store any data for purposes other than for performing the payment initiation service explicitly requested by the payment service user. Furthermore, Article 67 (2) (d) PSD2 limits the access of AISP to the information from designated payment accounts and associated payment transactions, whereas Article 67 (2) (f) PSD2 states that AISP shall not use, access or store any data for purposes other than for performing the account information service explicitly requested by the payment service user, in accordance with data protection rules. The latter emphasises that, within the context of the account information services, personal data can only be collected for specified, explicit and legitimate purposes. An AISP should therefore make explicit in the contract for what specific purposes personal account information data are going to be processed for, in the context of the account information service it provides. The contract should be lawful, fair and transparent under Article 5 of the GDPR and also comply with other consumer protection laws.
12. Depending on specific circumstances, payment service providers could be a controller or processor under the GDPR. In these guidelines, ‘controllers’ are those payment service providers who, alone or jointly with others, determine the purposes and means of the processing of personal data. More guidance on this can be found in the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

## 2 LAWFUL GROUNDS AND FURTHER PROCESSING UNDER THE PSD2

### 2.1 Lawful grounds for processing

13. Under the GDPR, controllers must have a legal basis in order to process personal data. Article 6 (1) of the GDPR constitutes an exhaustive and restrictive list of six legal bases for processing of personal data under the GDPR<sup>13</sup>. It is up to the controller to define the appropriate legal basis and ensure that all conditions for this legal basis are met. Determining which basis is valid and most appropriate in a specific situation depends on the circumstances under which the processing takes place, including the purpose of the processing and relationship between the controller and the data subject.

### 2.2 Article 6(1)(b) of the GDPR (processing is necessary for the performance of a contract)

14. Payment services are provided on a contractual basis between the payment services user and the payment services provider. As stated in recital 87 of the PSD2, "*[t]his Directive should concern only contractual obligations and responsibilities between the payment service user and the payment service provider.*" In terms of the GDPR, the main legal basis for the processing of personal data for the provision of payment services is Article 6(1)(b) of the GDPR, meaning that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

15. The payment services under the PSD2 are defined in annex 1 of the PSD2. The provision of these services as defined by the PSD2 is a requirement for the establishment of a contract in which parties have access to payment account data of the payment service user. These payment service providers also have to be licenced operators. In relation to payment initiation services and account information services under the PSD2, contracts may incorporate terms that also impose conditions about additional services that are not regulated by the PSD2. The *EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects* make clear that controllers have to assess what processing of personal data is objectively necessary to perform the contract. These Guidelines point out that the justification of the necessity is dependent on the nature of the service, the mutual perspectives

---

<sup>13</sup> According to Article 6 processing shall be lawful only if and to the extent that at least one of the following applies:

- (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

and expectations of the parties to the contract, the rationale of the contract and the essential elements of the contract.

16. The EDPB guidelines 2/2019 also make clear that, in light of Article 7(4) of the GDPR, a distinction is made between processing activities necessary for the performance of a contract and terms making the service conditional on certain processing activities that are not in fact necessary for the performance of the contract. ‘Necessary for performance’ clearly requires something more than a contractual condition<sup>14</sup>. The controller should be able to demonstrate how the main object of the specific contract with the data subject cannot, as a matter of fact, be performed if the specific processing of the personal data in question does not occur. Merely referencing or mentioning data processing in a contract is not enough to bring the processing in question within the scope of Article 6(1)(b) of the GDPR.
17. Article 5 (1) (b) of the GDPR provides for the purpose limitation principle, which requires that personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. When assessing whether Article 6(1)(b) is an appropriate legal basis for an online (payment) service, regard should be given to the particular aim, purpose, or objective of the service<sup>15</sup>. The purposes of the processing must be clearly specified and communicated to the data subject, in line with the controller’s purpose limitation and transparency obligations. Assessing what is ‘necessary’ involves a combined, fact-based assessment of the processing “for the objective pursued and of whether it is less intrusive compared to other options for achieving the same goal”. Article 6(1)(b) does not cover processing which is useful but not objectively necessary for performing the contractual service or for taking relevant pre-contractual steps at the request of the data subject, even if it is necessary for the controller’s other business purposes<sup>16</sup>.
18. The EDPB Guidelines 2/2019 make clear that contracts cannot artificially expand the categories of personal data or types of processing operation that the controller needs to carry out for the performance of the contract within the meaning of Article 6(1)(b)<sup>17</sup>. These Guidelines also address cases in which ‘take it or leave it’ situations may be created for data subjects who may only be interested in one of the services. This could happen when a controller wishes to bundle several separate services or elements of a service with different fundamental purposes, features or rationale into one contract. Where the contract consists of several separate services or elements of a service that can in fact reasonably be performed independently of one another, the applicability of Article 6(1)(b) should be assessed in the context of each of those services separately, looking at what is objectively necessary to perform each of the individual services which the data subject has actively requested or signed up for<sup>18</sup>.
19. In line with the abovementioned Guidelines, controllers have to assess what is objectively necessary for the performance of the contract. Where controllers cannot demonstrate that the processing of the personal payment account data is objectively necessary for the provision of each of these services separately, Article 6 (1) (b) of the GDPR is not a valid legal ground for processing. In these cases, the controller should consider another legal basis for processing.

---

<sup>14</sup> Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, EDPB, page 8.

<sup>15</sup> Idem.

<sup>16</sup> Idem, page 7.

<sup>17</sup> Idem, page 10.

<sup>18</sup> Idem, page 11.

### 2.3 Fraud prevention

20. Article 94 (1) PSD2 states that Member States shall permit processing of personal data by payment systems and payment service providers when necessary to safeguard the prevention, investigation and detection of payment fraud. The processing of personal data strictly necessary for the purposes of preventing fraud could constitute a legitimate interest of the payment service provider concerned, provided that such interests are not overridden by the interests or fundamental rights and freedoms of the data subject<sup>19</sup>. Processing activities for the purpose of fraud prevention should be based on a careful case by case evaluation by the controller, in accordance with the accountability principle. In addition, to prevent fraud, controllers may also be subject to specific legal obligations that necessitate the processing of personal data.

### 2.4 Further processing (AISP and PISP)

21. Article 6 (4) of the GDPR determines the conditions for the processing of personal data for a purpose other than that for which the personal data have been collected. More specifically, such further processing may take place, where it is based on a Union or Member State law, which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), where the data subject has given their consent or where the processing for a purpose other than that for which the personal data were collected is compatible with the initial purpose.
22. Articles 66 (3) (g) and 67 (2) (f) of the PSD2 have to be taken into careful consideration. As mentioned above, Article 66 (3) (g) of the PSD2 states that the PISP shall not use, access or store any data for purposes other than for the provision of the payment initiation service as explicitly requested by the payer. Article 67 (2) (f) of the PSD2 states that the AISP shall not use, access or store any data for purposes other than for performing the account information service explicitly requested by the payment service user, in accordance with data protection rules.
23. Consequently, Article 66(3)(g) and Article 67 (2) (f) of the PSD2 considerably restrict the possibilities for processing for other purposes, meaning that the processing for another purpose is not allowed, unless the data subject has given consent pursuant to Article 6(1)(a) of the GDPR or the processing is laid down by Union law or Member State law to which the controller is subject, pursuant to Article 6 (4) of the GDPR. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law, the restrictions laid down in Article 66(3)(g) and Article 67(2)(f) of the PSD2 make clear that any other purpose is not compatible with the purpose for which the personal data are initially collected. The compatibility test of Article 6(4) GDPR cannot result in a legal basis for processing.
24. Article 6 (4) of the GDPR allows for further processing based on Union or Member State law. For example, all PISPs and AISPs are obliged entities under Article 3 (2) (a) Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing of the anti-money laundering directive. These obliged entities are therefore compelled to apply the customer due diligence measures as specified in the directive. The personal data processed in connection with a

---

<sup>19</sup> Recital 47 GDPR.

PSD2 service are, therefore, further processed based on at least one legal obligation resting on the service provider<sup>20</sup>.

25. As mentioned in paragraph 20, Article 6 (4) of the GDPR indicates that the processing for a purpose other than that for which the personal data have been collected could be based on the data subject's consent, if all the conditions for consent under the GDPR are met. As set out above, the controller needs to demonstrate that it is possible to refuse or withdraw consent without detriment (recital 42 of the GDPR).

## 2.5 Lawful ground for granting access to the Account (ASPSPs)

26. As mentioned in paragraph 10, payment service users can exercise their right to make use of payment initiation and account information services. The obligations imposed on the Member States in Articles 66(1) and 67(1) of the PSD2 should be implemented in national law in order to guarantee the effective application of the right of the payment service user to benefit from the aforementioned payment services. The effective application of such rights would not be possible without the existence of a corresponding obligation on the ASPSP, typically a bank, to grant the payment service provider access to the account under the condition that it has fulfilled all requirements to get access to the account of the payment service user. Furthermore, Articles 66(5) and 67(4) of the PSD2 state clearly that the provision of payment initiation services and of account information services shall not be dependent on the existence of a contractual relationship between the PISP/AISP and the ASPSP.
27. The processing of personal data by the ASPSP consisting of granting access to the personal data requested by the PISP and AISP in order to perform their payment service to the payment service user is based on a legal obligation. In order to achieve the objectives of the PSD2, ASPSPs must provide the personal data for the PISPs' and AISPs' services, which is a necessary condition for PISPs and AISPs to provide their services and thus ensure the rights provided for in Articles 66(1) and 67(1) of the PSD2. Therefore, the applicable legal ground in this case is Article 6 (1) (c) of the GDPR.
28. As the GDPR has specified that processing based on a legal obligation should be clearly laid down by Union or Member State law (see Article 6 (3) of the GDPR), the obligation for ASPSPs to grant access should stem from the national law transposing the PSD2.

---

<sup>20</sup> Note that a thorough examination of the question whether the anti-money laundering directive meets the standard of Art. 6 (4) GDPR falls outside of the scope of this document.

### 3 EXPLICIT CONSENT

#### 3.1 Consent under the GDPR

29. Under the GDPR, consent serves as one of the six legal grounds for the lawfulness of processing of personal data. Article 4 (11) of the GDPR defines consent as “any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”. These four conditions, freely given, specific, informed, and unambiguous, are essential for the validity of consent. According to the EDPB Guidelines 05/2020 on consent under Regulation 2016/679, consent can only be an appropriate lawful basis if a data subject is offered control and a genuine choice with regard to accepting or declining the terms offered or declining them without detriment. When asking for consent, a controller has the duty to assess whether it will meet all the requirements to obtain valid consent. If obtained in full compliance with the GDPR, consent is a tool that gives data subjects control over whether or not personal data concerning them will be processed. If not, the data subject's control becomes illusory and consent will be an invalid legal basis for processing, rendering the processing activity unlawful<sup>21</sup>.
30. The GDPR also contains further safeguards in Article 7, which sets out that the data controller must be in a position to demonstrate that there had been valid consent at the time of processing. Also, the request for consent must be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Furthermore, the data subject must be informed of the right to withdraw consent at any time, in just as simple a way as it was to grant consent.
31. According to Article 9 GDPR, consent is one of the exceptions from the general prohibition for processing special categories of personal data. However, in such case the data subject's consent must be 'explicit'<sup>22</sup>.
32. According to the EDPB Guidelines 05/2020 on consent under Regulation 2016/679, explicit consent under the GDPR refers to the way consent is expressed by the data subject. It means that the data subject should give an express statement of consent for specific processing purpose(s). An obvious way to make sure consent is explicit would be to expressly confirm consent in a written statement. Where appropriate, the controller could make sure the written statement is signed by the data subject, in order to remove all possible doubt and potential lack of evidence in the future.
33. Under no circumstances can consent be inferred from potentially ambiguous statements or actions. A controller must also beware that consent cannot be obtained through the same motion as agreeing to a contract or accepting general terms and conditions of a service.

#### 3.2 Consent under the PSD2

34. The EDPB notes that the legal framework regarding explicit consent is complex, since both the PSD2 and the GDPR include the concept of 'explicit consent'. This leads to the question whether "explicit consent" as mentioned in Article 94 (2) PSD2 should be interpreted in the same way as explicit consent under the GDPR.

---

<sup>21</sup> Guidelines 05/2020 on consent under Regulation 2016/679, EDPB, para. 3.

<sup>22</sup> See also Opinion 15/2011 on the definition of consent (WP 187), pp. 6-8, and/or Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217), pp. 9, 10, 13 and 14.

### 3.2.1 Explicit consent under Article 94 (2) PSD2

35. The PSD2 includes a number of specific rules concerning the processing of personal data, in particular in Article 94 (1) of the PSD2, which determines that the processing of personal data for the purposes of the PSD2 must comply with EU data protection law. Furthermore, Article 94 (2) of the PSD2 sets out that payment service providers shall only access, process and retain personal data necessary for the provision of their payment services, with the explicit consent of the payment service user. Pursuant to Article 33 (2) of the PSD2, this requirement of the explicit consent of the payment service user does not apply to AISPs. However, Article 67 (2)(a) of the PSD2 still provides for explicit consent for AISPs for the provision of the service.
36. As mentioned above, the list of lawful bases for processing under the GDPR is exhaustive. As mentioned in paragraph 14, the legal basis for the processing of personal data for the provision of payment services is, in principle, Article 6(1)(b) of the GDPR, meaning that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. From that, it follows that Article 94 (2) of the PSD2 cannot be regarded as an additional legal basis for processing of personal data. The EDPB considers that, in view of the foregoing, this paragraph should be interpreted, on the one hand, in coherence with the applicable data protection legal framework and, on the other hand, in a way that preserves its useful effect. Explicit consent under Article 94(2) PSD2 should therefore be regarded as an additional requirement of a contractual nature<sup>23</sup> in relation to the access to and subsequently processing and storage of personal data for the purpose of providing payment services and is therefore not the same as (explicit) consent under the GDPR.
37. “Explicit consent” referred to in Article 94 (2) PSD2 is a contractual consent. This implies that Article 94 (2) PSD2 should be interpreted in the sense that when entering a contract with a payment service provider under the PSD2, data subjects must be made fully aware of the specific categories of personal data that will be processed. Further, they have to be made aware of the specific (payment service) purpose for which their personal data will be processed and have to explicitly agree to these clauses. Such clauses should be clearly distinguishable from the other matters dealt with in the contract and would need to be explicitly accepted by the data subject.
38. Central to the notion of “explicit consent” under Article 94 (2) of the PSD2 is the gaining of access to personal data to subsequently process and store these data for the purpose of providing payment services. This implies that the payment service<sup>24</sup> provider is not yet processing the personal data, but needs access to personal data that have been processed under the responsibility of any other controller. If a payment service user enters into a contract with, for example, a payment initiation service provider, this provider needs to obtain access to personal data of the payment service user that is being processed under the responsibility of the account servicing payment service provider. The object of the explicit consent under Article 94 (2) PSD2 is the permission to obtain access to those personal data, to be able to process and store these personal data that are necessary for the purpose of providing the payment service. If explicit consent is given by the data subject, the account servicing payment service provider is obliged to give access to the indicated personal data.
39. Although the consent of Article 94 (2) of the PSD2 is not a legal ground for the processing of personal data, this consent is specifically related to personal data and data protection, and ensures

---

<sup>23</sup> Letter of the EDPB regarding the PSD2 directive, 5 July 2018, page 4.

<sup>24</sup> This applies to services 1 to 7 of Annex 1 of the PSD2.

transparency and a degree of control for the payment service user<sup>25</sup>. While the PSD2 does not specify the substantive conditions for consent under Article 94 (2) PSD2, it should, as stated above, be understood in coherence with the applicable data protection legal framework and in a way that preserves its useful effect.

40. With regard to the information to be provided by controllers and the requirement of transparency, Article 29 Working Party Guidelines on Transparency specifies that a “*A central consideration of the principle of transparency outlined in these provisions is that the data subject should be able to determine in advance what the scope and consequences of the processing entails and that they should not be taken by surprise at a later point about the ways in which their personal data has been used*”<sup>26</sup>.
41. Furthermore, as required by the principle of purpose limitation, personal data must be collected for specified, explicit and legitimate purposes (Article 5 (1) (b) of the GDPR). Where personal data are collected for more than one purpose, “*controllers should avoid identifying only one broad purpose in order to justify various further processing activities which are in fact only remotely related to the actual initial purpose*”<sup>27</sup>. The EDPB has highlighted, most recently in the context of contracts for online services, the risk of inclusion of general processing terms in contracts and has stated that the purpose of the collection should be clearly and specifically identified: it should be detailed enough to determine what kind of processing is and is not included within the specified purpose, and to allow that compliance with the law can be assessed and data protection safeguards applied<sup>28</sup>.
42. When considered in the context of the additional requirement of explicit consent pursuant to Article 94(2) of the PSD2, this entails that controllers must provide data subjects with specific and explicit information about the specific purposes identified by the controller for which their personal data are accessed, processed and retained. In line with Article 94(2) of the PSD2, the data subjects must explicitly accept these specific purposes.
43. Furthermore, as set out above in paragraph 10, the EDPB highlights that the payment service user must be able to choose whether or not to use the service and cannot be forced to do so. Therefore, the consent under Article 94 (2) of the PSD2 also has to be a freely given consent.

### 3.3 Conclusion

44. Explicit consent under the PSD2 is different from (explicit) consent under the GDPR. Explicit consent under Article 94 (2) of the PSD2 is an additional requirement of a contractual nature. When a payment service provider needs access to personal data for the provision of a payment service, explicit consent in line with Article 94 (2) of the PSD2 of the payment service user is needed.

---

<sup>25</sup> Art. 94 (2) PSD2 falls under Chapter 4 ‘Data protection’.

<sup>26</sup> Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, paragraph 10 (adopted on 11 April 2018) - endorsed by the EDPB.

<sup>27</sup> Article 29 Working Party Opinion 03/2013 on purpose limitation (WP203), page 16.

<sup>28</sup> Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, paragraph 16 (public consultation version) and Article 29 Working Party Opinion 03/2013 on purpose limitation (WP203), page 15–16.

## 4 THE PROCESSING OF SILENT PARTY DATA

### 4.1 Silent party data

45. A data protection issue that needs careful consideration, is the processing of so called ‘silent party data’. In the context of this document, silent party data are personal data concerning a data subject who is not the user of a specific payment service provider, but whose personal data are processed by that specific payment service provider for the performance of a contract between the provider and the payment service user. This is for example the case where a payment service user, data subject A, makes use of the services of an AISPs, and data subject B has made a series of payment transactions to the payment account of data subject A. In this case, data subject B is regarded as the ‘silent party’ and the personal data (such as the account number of data subject B and the amount of money that was involved in these transactions) relating to data subject B, is regarded as ‘silent party data’.

### 4.2 The legitimate interest of the controller

46. Article 5 (1) (b) GDPR requires that personal data are only collected for specified, explicit and legitimate purposes and may not be further processed in a manner that is incompatible with those purposes. In addition, the GDPR requires that that any processing of personal data must be both necessary as well as proportionate and in line with the data protection principles, such as those of purpose limitation and data minimisation.

47. The GDPR may allow for the processing of silent party data when this processing is necessary for purposes of the legitimate interests pursued by a controller or by a third party (Article 6 (1)(f) GDPR). However, such processing can only take place when the legitimate interest of the controller is not “overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data”.

48. A lawful basis for the processing of silent party data by PISPs and AISPs - in the context of the provision of payment services under the PSD2 - could thus be the legitimate interest of a controller or a third party to perform the contract with the payment service user. The necessity to process personal data of the silent party is limited and determined by the reasonable expectations of these data subjects. In the context of providing payment services that are covered by the PSD2, effective and appropriate measures have to be established to safeguard that the interests or fundamental rights and freedoms of the silent parties are not overridden, and to ensure that the reasonable expectations of these data subjects regarding the processing of their personal data are respected. In this respect, the controller (AISP or PISP) has to establish the necessary safeguards for the processing in order to protect the rights of data subjects. This includes technical measures to ensure that silent party data are not processed for a purpose other than the purpose for which the personal data were originally collected by PISPs and AISPs. If feasible, also encryption or other techniques should be applied to achieve an appropriate level of security and data minimisation.

### 4.3 Further processing of personal data of the silent party

49. As stated under paragraph 29, personal data processed in connection with a payment service regulated by the PSD2, could be further processed based on legal obligations resting on the service provider. These legal obligations could concern personal data of the silent party.

50. With regard to further processing of silent party data on the basis of legitimate interest, the EDPB is of the opinion that these data cannot be used for a purpose other than that for which the personal data have been collected, other on the basis of EU or Member State law. Consent of the

silent party is legally not feasible, because in order to obtain consent, personal data of the silent party would have to be collected or processed, for which no legal ground can be found under Article 6 GDPR. The compatibility test of Article 6.4 of the GDPR cannot offer a ground for the processing for other purposes (e.g. direct marketing activities) either. The rights and freedoms of these silent party data subjects will not be respected if the new data controller uses the personal data for other purposes, taking into account the context in which the personal data have been collected, especially the absence of any relationship with the data subjects that are silent parties<sup>29</sup>; the absence of any connection between any other purpose and the purpose for which the personal data were initially collected (i.e. the fact that PSPs only need the silent party data in order to perform a contract with the other contracting party); the nature of the personal data involved<sup>30</sup>, the circumstance that data subjects are not in a position to reasonably expect any further processing or to even be aware which controller may be processing their personal data and given the legal restrictions on processing set out in Article 66 (3) (g) and Article 67 (2) (f) of PSD2.

---

<sup>29</sup> Recital 87 of PSD2 states that PSD2 only concerns ‘contractual obligations and responsibilities between the payment service user and the payment service provider’. Silent Party Data therefore do not fall under the scope of PSD2.

<sup>30</sup> Particular care should be taken when processing financial personal data, as the processing can be considered as increasing the possible risk to the rights and freedoms of individuals, according to the Guidelines on Data Protection Impact Assessment (DPIA).

## 5 THE PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA UNDER THE PSD2

### 5.1 Special categories of personal data

51. Article 9 (1) GDPR prohibits the processing of “personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation”.
52. It should be emphasised that in some Member States, electronic payments are already ubiquitous, and are favoured by many people over cash in their day to day transactions. At the same time, financial transactions can reveal sensitive information about an individual data subject, including those related to special categories of personal data. For example, depending on the transaction details, political opinions and religious beliefs may be revealed by donations made to political parties or organisations, churches or parishes. Trade union membership may be revealed by the deduction of an annual membership fee from a person's bank account. Personal data concerning health may be gathered from analysing medical bills paid by a data subject to a medical professional (for instance a psychiatrist). Finally, information on certain purchases may reveal information concerning a person's sex life or sexual orientation. As shown by these examples, even single transactions can contain special categories of personal data. Moreover, account information services might rely on profiling as defined by article 4 (4) of the GDPR. As previously stated in the Working Party 29 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, as endorsed by the EDPB , “profiling can create special category of data by inference from data which is not special category of data in its own right, but becomes so when combined with other data.”<sup>31</sup> This means that, through the sum of financial transactions, different kinds of behavioural patterns can be revealed, which may include special categories of personal data. Therefore, the chances are considerable that a service provider processing information on financial transactions of data subjects also processes special categories of personal data.
53. With regard to the term ‘sensitive payment data’, the EDPB notes the following. The definition of sensitive payment data in the PSD2 differs considerably from the way the term ‘sensitive personal data’ is commonly used within the context of the GDPR and data protection (law). Where the PSD2 defines ‘sensitive payment data’ as ‘data, including personalized security credentials which can be used to carry out fraud’, the GDPR emphasises the need for specific protection of special categories of personal data which under Article 9 of the GDPR are, by their nature, particularly sensitive in relation to fundamental rights and freedoms, such as special categories of personal data<sup>32</sup>. In this regard it is recommended to at least map out and categorize precisely what kind of personal data will be processed. Most probably a Data Protection Impact Assessment (DPIA) will be required in accordance with article 35 GDPR, which will help in this mapping exercise. More guidance on DPIAs can be found in the Working Party 29 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation

---

<sup>31</sup> Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01, page 15.

<sup>32</sup> For example, in recital 10 of the GDPR, special categories of personal data are being referred to as ‘sensitive data’.

2016/679, as endorsed by the EDPB.

## 5.2 Possible derogations

54. The prohibition of Article 9 GDPR is not absolute. In particular, whereas derogations of paragraphs (b)-(f) and (h)-(j) of Article 9 (2) GDPR are manifestly not applicable to the processing of personal data in the PSD2 context, the following two derogations in Article 9 (2) GDPR could be considered:
- a) The prohibition does not apply if the data subject has given explicit consent to the processing of those personal data for one or more specified purposes (Article 9 (2) (a) GDPR).
  - b) The prohibition does not apply if the processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject (Article 9 (2) (g) GDPR).
55. It should be pointed out that the list of derogations in Article 9 (2) GDPR is exhaustive. The possibility that special categories of personal data are included in the personal data processed for the provision of any of the services falling under the PSD2 must be recognised by the service provider. As the prohibition of Article 9 (1) GDPR is applicable to these service providers, they must ensure that one of the exceptions in Article 9 (2) GDPR is applicable to them. It should be emphasised that where the service provider cannot show that one of the derogations is met, the prohibition of article 9 (1) is applicable.

## 5.3 Substantial public interest

56. Payments services may process special categories personal data for reasons of substantial public interest, but only when all the conditions of Article 9 (2) (g) of the GDPR are met. This means that the processing of the special categories of personal data has to be addressed in a specific derogation to article 9 (1) GDPR in Union or Member State law. This provision will have to address the proportionality in relation to the pursued aim of the processing and contain suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. Furthermore, this provision under Union or Member State law will have to respect the essence of the right to data protection. Finally, the processing of the special categories of data must also be demonstrated to be necessary for the reason of the substantial public interest, including interests of systemic importance. Only when all of these conditions are fully met, this derogation could be made applicable to designated types of payment services.

## 5.4 Explicit consent

57. In cases where the derogation of article 9 (2) (g) GDPR does not apply, obtaining explicit consent in accordance with the conditions for valid consent in the GDPR, seems to remain the only possible lawful derogation to process special categories of personal data by TPPs. The EDPB Guidelines 05/2020 on consent under Regulation 2016/679 states<sup>33</sup> that: “Article 9(2) does not recognize “necessary for the performance of a contract” as an exception to the general prohibition to process special categories of data. Therefore, controllers and Member States that deal with this situation should explore the specific exceptions in Article 9(2) subparagraphs (b) to (j). When service providers rely on Article 9 (2) (a) GDPR, they must ensure that they have been granted explicit

---

<sup>33</sup> Guidelines 05/2020 on consent under Regulation 2016/679, EDPB, para. 99

consent before commencing the processing.” Explicit consent as set out in Article 9 (2) (a) GDPR must meet all the requirements of the GDPR.

### 5.5 No suitable derogation

58. As noted above, where the service provider cannot show that one of the derogations is met, the prohibition of Article 9 (1) is applicable. In this case technical measures could be put in place to prevent the processing of special categories of personal data, for instance by preventing the processing of certain data points. In this respect, payment service providers may explore the technical possibilities to exclude special categories of personal data and allow a selected access which would prevent the processing of special categories of personal data related to silent parties by TPPs.

## 6 DATA MINIMISATION, SECURITY, TRANSPARANCY, ACCOUNTABILITY AND PROFILING

### 6.1 Data minimisation and data protection by design and default

59. The principle of data minimisation is enshrined in Article 5 (1) (c) GDPR: “Personal data shall be [...] adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed”. Essentially, under the principle of data minimisation, controllers should process no more personal data than what is necessary in order to achieve the specific purpose in question. As pointed out in Chapter 2, the amount and the kind of personal data necessary to provide the payment service is determined by the objective and mutually understood contractual purpose<sup>34</sup>. Data minimisation is applicable to every processing (e.g. every collection of or access to and request of personal data). The EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (DPbDD), state that ‘processors and technology providers are also recognised as key enablers for DPbDD, they should also be aware that controllers are required to only process personal data with systems and technologies that have built-in data protection<sup>35</sup>’.
60. Article 25 of the GDPR contains the obligations to apply data protection by design and by default. These obligations are of particular importance to the principle of data minimisation. This Article determines that controllers shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, which are designed to implement data protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects. 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. These measures may include encryption, pseudonymisation and other technical measures.
61. When the obligation of article 25 of the GDPR is applied, the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing are the elements that have to be taken into account. Further clarifications about this obligation are given in the abovementioned EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.

### 6.2 Data minimisation measures

62. The TPP accessing payment account data in order to provide the requested services must also take the principle of data minimisation into account and must only collect personal data necessary to provide the specific payment services requested by the payment service user. As a principle, the access to the personal data should be limited to what is necessary for the provision of payment services. As has been shown in Chapter 2, the PSD2 requires ASPSPs to share payment service user information on request of the payment service user, when the payment service user wishes to use a payment initiation service or an account information service.

---

<sup>34</sup> Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, EDPB, para 32

<sup>35</sup> Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, page 29.

63. When not all payment account data are necessary for the provision of the contract, a selection of the relevant data categories should be made by the AISP before the data are collected. For instance, data categories that may not be necessary may include the identity of the silent party and the transaction characteristics. Also, unless required by Member State or EU law, the IBAN of the silent party's bank account may not need to be displayed.
64. In this respect, the possible application of technical measures that enable or support TPPs in their obligation to access and retrieve only the personal data necessary for the provision of their services could be considered, as part of the implementation of appropriate data protection policies, in line with article 24 (2) GDPR. In this respect, the EDPB recommends the usage of digital tools in order to support AISPs in their obligation to only collect personal data that are necessary for the purposes for which they are processed. For instance, when a service provider does not need the transaction characteristics (in the description field of the transaction records) for the provision of their service, a digital selection tool could function as a means for TPPs to exclude this field from the overall processing operations by the TPP.

**Example 2:**

HappyPayments, our Account Information Service provider from example 1, wants to ensure that it only processes the personal payment account data which its users are interested in. To seek access to more payment account data would not be necessary for the provision of the service. Therefore, it allows the users to select the specific types of information they are interested in.

User A wants an overview of its spending for the last two months. Thus, it asks for its two banking accounts, held with two different ASPSPs, the information on all transactions of the last two months, the transaction amount, the date of execution and the recipient's name, and ticks the corresponding boxes in HappyPayments' user interface.

HappyPayments then commences to request from the respective ASPSPs only the information corresponding to the fields set by User A and only for the period of the last two months. Information such as the "communication" of the transfer or even the IBAN are not requested, as User A did not ask for this information.

To allow HappyPayments to comply with its data minimisation obligations, the ASPSPs allow HappyPayments to request specific fields for a range of dates.

65. It should also be noted in this regard that under the PSD2, ASPSPs are only allowed to provide access to payment account information. There is no legal basis under the PSD2 to provide access with regard to personal data contained in other accounts, such as savings, mortgages or investment accounts. Accordingly, under the PSD2, technical measures have to be implemented to ensure that access is limited to the necessary payment account information.
66. Besides collecting as little data as possible, the service provider also has to implement limited retention periods. Personal data should not be stored by the service provider for a period longer than is necessary in relation to the purposes requested by the payment service user.
67. If the contract between the data subject and the AISP requires the transmission of personal data to third parties, then only those personal data that are necessary for the execution of the contract can be transmitted. Data subjects should also be specifically informed about the transmission and the personal data that are going to be transmitted to this third party.

### 6.3 Security

68. The EDPB already highlighted that the violation of financial personal data “*clearly involves serious impacts in the data subject’s daily life*” and quotes the risks of payment fraud as an example<sup>36</sup>.
69. Where a data breach involves financial data, the data subject may be exposed to considerable risks. Depending on the information that is leaked, data subjects may be exposed to a risk of identity theft, of theft of the funds in their accounts and other assets. Furthermore, there is the possibility that the exposure of transaction data is related to considerable privacy risks, as transaction data may contain references to all aspects of a data subject’s private life. At the same time, financial data are obviously valuable to criminals and therefore an attractive target.
70. As controllers, payment service providers are obligated to take adequate measures to protect the personal data of data subjects (Article 24 (1) GDPR). The higher the risks associated with the processing activity carried out by the controller, the higher the security standards that need to be applied. As the processing of financial data is connected to a variety of severe risks, the security measures should be accordingly high.
71. Service providers should be held to high standards, including strong customer authentication mechanisms and high security standards for the technical equipment<sup>37</sup>. Other procedures, such as vetting processors for security standards and implementing procedures against unauthorised access, are also important.

#### 6.4 Transparency and accountability

72. Transparency and accountability are two fundamental principles of the GDPR.
73. With regard to transparency (Article 5 (1)(a) of the GDPR), Article 12 of the GDPR specifies that controllers shall take appropriate measures to provide any information referred to in Articles 13 and 14 GDPR. Furthermore, it requires that the information or communication about the processing of personal data must be concise, transparent, intelligible and easily accessible. The information must be in clear and plain language and in writing “or by other means, including where appropriate, by electronic means”. The Article 29 Working Party ‘Guidelines on transparency under Regulation 2016/679’, as endorsed by the EDPB, offers specific guidance for compliance with the principle of transparency in digital environments.
74. According to the abovementioned Guidelines on transparency under Regulation 2016/679, Article 11 GDPR should be interpreted as a way of enforcing genuine data minimisation without hindering the exercise of data subject rights, and that the exercise of data subject rights should be made possible with the help of additional information provided by the data subject. There may be situations where a data controller is processing personal data which does not require the identification of a data subject (for example with pseudonymised data). In such cases, Article 11.1 may also be relevant as it states that a data controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purposes of complying with the GDPR.
75. For the services under the PSD2, Article 13 GDPR is applicable for the personal data collected from the data subject and Article 14 is applicable where personal data have not been obtained from the data subject.

---

<sup>36</sup> Article 29 Working Party Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, WP248 rev.01 - endorsed by the EDPB.

<sup>37</sup> See the RTS.

76. In particular, the data subject has to be informed about the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period, and where applicable, the legitimate interests pursued by the controller or by a possible third party. Where processing is based on consent as referred to in Article 6(1) (a) GDPR or explicit consent as referred to in Article 9(2) (a) GDPR, the data subject has to be informed of the existence of the right to withdraw consent at any time.
77. The controller shall provide the information to the data subject, having regard to the specific circumstances in which the personal data are processed. If the personal data are to be used for communication with the data subject<sup>38</sup>, which will probably will be the case for AISPs, the information has to be provided at the latest at the time of the first communication to that data subject. If personal data are to be disclosed to another recipient, the information has to be provided at the latest when the personal data are first disclosed.
78. With regard to online payment services, the abovementioned Guidelines clarify that a layered approach may be followed by data controllers where they opt to use a combination of methods to ensure transparency. It is particularly recommended that layered privacy statements/ notices should be used to link to the various categories of information which must be provided to the data subject, rather than displaying all such information in a single notice on a screen, in order to avoid information fatigue, and at the same time ensuring the effectiveness of the information.
79. The abovementioned Guidelines also clarify that controllers may choose to use additional tools to provide information to the individual data subject, such as privacy dashboards. A privacy dashboard is a single point from which data subjects can view ‘privacy information’ and manage their privacy preferences by allowing or preventing their data from being used in certain ways by the controller in question<sup>39</sup>. A privacy dashboard could provide an overview of the TPPs that have obtained the data subjects explicit consent, and could also offer relevant information on the nature and amount of personal data that has been accessed by TPPs. In principle, an ASPSP may offer the user the possibility to withdraw a specific explicit PSD2 consent<sup>40</sup> through the overview, which would result in a denial of access to their payment accounts to one or more TPPs. The user could also request an ASPSP to deny access to their payment account(s) to one or more particular TPPs<sup>41</sup>, as it is the right of the user to (not) make use of an account information service. If privacy dashboards are used in order to give or withdraw an explicit consent, they should be designed and applied lawfully and in particular prevent creating obstacles to the TPPs right to provide services in accordance with the PSD2. In this respect and in accordance with the applicable provisions under the PSD2, a TPP has the possibility to obtain explicit consent from the user again after this consent has been withdrawn.
80. The accountability principles requires the controller to lay down appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in

---

<sup>38</sup> Art. 14 (3) (b) of the GDPR.

<sup>39</sup> According to the Article 29 Working Party Guidelines on transparency under Regulation 2016/679 - endorsed by the EDPB, privacy dashboards are particularly useful when the same service is used by data subjects on a variety of different devices as they give them access to and control over their personal data no matter how they use the service. Allowing data subjects to manually adjust their privacy settings via a privacy dashboard can also make it easier for a privacy statement/ notice to be personalised by reflecting only the types of processing occurring for that particular data subject.

<sup>40</sup> See for example the ‘explicit consent’ mentioned in Article 67 (2) (a) of the PSD2.

<sup>41</sup> See also EBA/OP/2020/10, paragraph 45

accordance with the GDPR, in particular with the main data protection principles provided for by Article 5 (1). Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons, and must be reviewed and updated when necessary<sup>42</sup>.

## 6.5 Profiling

81. The processing of personal data by payment service providers may entail ‘profiling’ as referred to in Article 4 (4) of the GDPR. For example, AISPs could rely on automated processing of personal data in order to evaluate certain personal aspects relating to a natural person. A data subject’s personal financial situation could be evaluated, depending on the specifics of the service. Account information services, to be provided as requested by users, may involve an extensive evaluation of personal payment account data.
82. The controller also has to be transparent to the data subject on the existence of automated decision-making, including profiling. In those cases, the controller has to provide meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject (Article 13(2) (f) and Article 14 (2) (g) and recital 60)<sup>43</sup>. Likewise, under Article 15 of the GDPR the data subject has the right to request and obtain information from the controller about the existence of automated decision-making, including profiling, the logic involved and the consequences for the data subject, and, in certain circumstances, a right to object to profiling, regardless of whether solely automated individual decision-making based on profiling takes place<sup>44</sup>.
83. Furthermore, what is also relevant in this context is the right of the data subject not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affecting him or her, provided for by Article 22 of GDPR. This norm also includes, in certain circumstances, the need for data controllers to implement suitable measures to safeguard the data subject’s rights such as specific information to the data subject, the right to obtain human intervention in the decision making and to express his or her point of view and contest the decision. As also stated in recital 71 of GDPR this means, inter alia, that data subjects have the right not to be subject to a decision, such as automatic refusal of an online credit application without any human intervention<sup>45</sup>.
84. Automated decision-making, including profiling that involves special categories of personal data is only allowed under the cumulative conditions of Article 22(4) GDPR:
- there is an applicable Article 22(2) exemption;
  - and paragraph (a) or (g) of Article 9(2) GDPR applies. In both cases, the controller shall put in place suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests<sup>46</sup>.
85. The requirements for further processing, as stated in these guidelines, should also be observed. The clarifications and instructions on automated individual decision-making and profiling given by

---

<sup>42</sup> Art. 5(2) and Art. 24 GDPR.

<sup>43</sup> Guidelines on transparency under Regulation 2016/679, WP 260 rev.01 - endorsed by the EDPB

<sup>44</sup> Article 29 Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01

<sup>45</sup> Recital 71 GDPR.

<sup>46</sup> Article 29 Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01, page 24.

the Working Party 29 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, as endorsed by the EDPB, are fully relevant in the context of payment services and should therefore be duly considered.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

# Guidelines



**Guidelines 07/2020 on the concepts of controller and processor in the GDPR**

**Version 2.1**

**Adopted on 07 July 2021**

## Version history

Version 2.1	20 September 2022	Minor corrections
Version 2.0	7 July 2021	Adoption of the Guidelines after public consultation
Version 1.0	2 September 2020	Adoption of the Guidelines for public consultation

## EXECUTIVE SUMMARY

The concepts of controller, joint controller and processor play a crucial role in the application of the General Data Protection Regulation 2016/679 (GDPR), since they determine who shall be responsible for compliance with different data protection rules, and how data subjects can exercise their rights in practice. The precise meaning of these concepts and the criteria for their correct interpretation must be sufficiently clear and consistent throughout the European Economic Area (EEA).

The concepts of controller, joint controller and processor are *functional* concepts in that they aim to allocate responsibilities according to the actual roles of the parties and *autonomous* concepts in the sense that they should be interpreted mainly according to EU data protection law.

### Controller

In principle, there is no limitation as to the type of entity that may assume the role of a controller but in practice it is usually the organisation as such, and not an individual within the organisation (such as the CEO, an employee or a member of the board), that acts as a controller.

A controller is a body that *decides* certain key elements of the processing. Controllership may be defined by law or may stem from an analysis of the factual elements or circumstances of the case. Certain processing activities can be seen as naturally attached to the role of an entity (an employer to employees, a publisher to subscribers or an association to its members). In many cases, the terms of a contract can help identify the controller, although they are not decisive in all circumstances.

A controller determines the purposes and means of the processing, i.e. the *why* and *how* of the processing. The controller must decide on both purposes and means. However, some more practical aspects of implementation (“non-essential means”) can be left to the processor. It is not necessary that the controller actually has access to the data that is being processed to be qualified as a controller.

### Joint controllers

The qualification as joint controllers may arise where more than one actor is involved in the processing. The GDPR introduces specific rules for joint controllers and sets a framework to govern their relationship. The overarching criterion for joint controllership to exist is the joint participation of two or more entities in the determination of the purposes and means of a processing operation. Joint participation can take the form of a *common decision* taken by two or more entities or result from *converging decisions* by two or more entities, where the decisions complement each other and are necessary for the processing to take place in such a manner that they have a tangible impact on the determination of the purposes and means of the processing. An important criterion is that the processing would not be possible without both parties’ participation in the sense that the processing by each party is inseparable, i.e. inextricably linked. The joint participation needs to include the determination of purposes on the one hand and the determination of means on the other hand.

### Processor

A processor is a natural or legal person, public authority, agency or another body, which processes personal data on behalf of the controller. Two basic conditions for qualifying as processor exist: that it is a separate entity in relation to the controller and that it processes personal data on the controller’s behalf.

The processor must not process the data otherwise than according to the controller’s instructions. The controller’s instructions may still leave a certain degree of discretion about how to best serve the

controller's interests, allowing the processor to choose the most suitable technical and organisational means. A processor infringes the GDPR, however, if it goes beyond the controller's instructions and starts to determine its own purposes and means of the processing. The processor will then be considered a controller in respect of that processing and may be subject to sanctions for going beyond the controller's instructions.

#### Relationship between controller and processor

A controller must only use processors providing sufficient guarantees to implement appropriate technical and organisational measures so that the processing meets the requirements of the GDPR. Elements to be taken into account could be the processor's expert knowledge (e.g. technical expertise with regard to security measures and data breaches); the processor's reliability; the processor's resources and the processor's adherence to an approved code of conduct or certification mechanism.

Any processing of personal data by a processor must be governed by a contract or other legal act which shall be in writing, including in electronic form, and be binding. The controller and the processor may choose to negotiate their own contract including all the compulsory elements or to rely, in whole or in part, on standard contractual clauses.

The GDPR lists the elements that have to be set out in the processing agreement. The processing agreement should not, however, merely restate the provisions of the GDPR; rather, it should include more specific, concrete information as to how the requirements will be met and which level of security is required for the personal data processing that is the object of the processing agreement.

#### Relationship among joint controllers

Joint controllers shall in a transparent manner determine and agree on their respective responsibilities for compliance with the obligations under the GDPR. The determination of their respective responsibilities must in particular regard the exercise of data subjects' rights and the duties to provide information. In addition to this, the distribution of responsibilities should cover other controller obligations such as regarding the general data protection principles, legal basis, security measures, data breach notification obligation, data protection impact assessments, the use of processors, third country transfers and contacts with data subjects and supervisory authorities.

Each joint controller has the duty to ensure that they have a legal basis for the processing and that the data are not further processed in a manner that is incompatible with the purposes for which they were originally collected by the controller sharing the data.

The legal form of the arrangement among joint controllers is not specified by the GDPR. For the sake of legal certainty, and in order to provide for transparency and accountability, the EDPB recommends that such arrangement be made in the form of a binding document such as a contract or other legal binding act under EU or Member State law to which the controllers are subject.

The arrangement shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects and the essence of the arrangement shall be made available to the data subject.

Irrespective of the terms of the arrangement, data subjects may exercise their rights in respect of and against each of the joint controllers. Supervisory authorities are not bound by the terms of the arrangement whether on the issue of the qualification of the parties as joint controllers or the designated contact point.

## TABLE OF CONTENTS

EXECUTIVE SUMMARY .....	3
INTRODUCTION .....	7
<b>PART I – CONCEPTS.....</b>	<b>8</b>
1    GENERAL OBSERVATIONS.....	8
2    DEFINITION OF CONTROLLER .....	9
2.1    Definition of controller .....	9
2.1.1    “Natural or legal person, public authority, agency or other body” .....	10
2.1.2    “Determines” .....	11
2.1.3    “Alone or jointly with others”.....	14
2.1.4    “Purposes and means” .....	14
2.1.5    “Of the processing of personal data”.....	17
3    DEFINITION OF JOINT CONTROLLERS .....	18
3.1    Definition of joint controllers .....	18
3.2    Existence of joint controllership .....	18
3.2.1    General considerations.....	18
3.2.2    Assessment of joint participation .....	19
3.2.3    Situations where there is no joint controllership.....	24
4    DEFINITION OF PROCESSOR .....	25
5    DEFINITION OF THIRD PARTY/RECIPIENT .....	28
<b>PART II – CONSEQUENCES OF ATTRIBUTING DIFFERENT ROLES.....</b>	<b>30</b>
1    RELATIONSHIP BETWEEN CONTROLLER AND PROCESSOR .....	30
1.1    Choice of the processor .....	30
1.2    Form of the contract or other legal act .....	31
1.3    Content of the contract or other legal act .....	34
1.3.1    The processor must only process data on documented instructions from the controller (Art. 28(3)(a) GDPR).....	35
1.3.2    The processor must ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality (Art. 28(3)(b) GDPR).....	36
1.3.3    The processor must take all the measures required pursuant to Article 32 (Art. 28(3)(c) GDPR) .....	37
1.3.4    The processor must respect the conditions referred to in Article 28(2) and 28(4) for engaging another processor (Art. 28(3)(d) GDPR).....	37

1.3.5	The processor must assist the controller for the fulfilment of its obligation to respond to requests for exercising the data subject's rights (Article 28(3) (e) GDPR). ....	38
1.3.6	The processor must assist the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 (Art. 28(3)(f) GDPR). ....	38
1.3.7	On termination of the processing activities, the processor must, at the choice of the controller, delete or return all the personal data to the controller and delete existing copies (Art. 28(3)(g) GDPR).....	40
1.3.8	The processor must make available to the controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller (Art. 28(3)(h) GDPR).....	40
1.4	Instructions infringing data protection law .....	41
1.5	Processor determining purposes and means of processing.....	42
1.6	Sub-processors .....	42
2	CONSEQUENCES OF JOINT CONTROLLERSHIP .....	43
2.1	Determining in a transparent manner the respective responsibilities of joint controllers for compliance with the obligations under the GDPR.....	43
2.2	Allocation of responsibilities needs to be done by way of an arrangement .....	46
2.2.1	Form of the arrangement .....	46
2.2.2	Obligations towards data subjects.....	46
2.3	Obligations towards data protection authorities.....	48

## **The European Data Protection Board**

Having regard to Article 70 (1e) 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” or “the Regulation”),

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<sup>1</sup>,

Having regard to Article 12 and Article 22 of its Rules of Procedure,

Whereas the preparatory work of these guidelines involved the collection of inputs from stakeholders, both in writing and at a stakeholder event, in order to identify the most pressing challenges;

## **HAS ADOPTED THE FOLLOWING GUIDELINES**

### **INTRODUCTION**

1. This document seeks to provide guidance on the concepts of controller and processor based on the GDPR’s rules on definitions in Article 4 and the provisions on obligations in chapter IV. The main aim is to clarify the meaning of the concepts and to clarify the different roles and the distribution of responsibilities between these actors.
2. The concept of controller and its interaction with the concept of processor play a crucial role in the application of the GDPR, since they determine who shall be responsible for compliance with different data protection rules, and how data subjects can exercise their rights in practice. The GDPR explicitly introduces the accountability principle, i.e. the controller shall be responsible for, and be able to demonstrate compliance with, the principles relating to processing of personal data in Article 5. Moreover, the GDPR also introduces more specific rules on the use of processor(s) and some of the provisions on personal data processing are addressed - not only to controllers - but also to processors.
3. It is therefore of paramount importance that the precise meaning of these concepts and the criteria for their correct use are sufficiently clear and shared throughout the European Union and the EEA.
4. The Article 29 Working Party issued guidance on the concepts of controller/processor in its opinion 1/2010 (WP169)<sup>2</sup> in order to provide clarifications and concrete examples with respect to these concepts. Since the entry into force of the GDPR, many questions have been raised regarding to what extent the GDPR brought changes to the concepts of controller and processor and their respective roles. Questions were raised in particular to the substance and implications of the concept of joint controllership (e.g. as laid down in Article 26 GDPR) and to the specific obligations for processors laid down in Chapter IV (e.g. as laid down in Article 28 GDPR). Therefore, and as the EDPB recognizes that the concrete application of the concepts needs further clarification, the EDPB now deems it necessary

---

<sup>1</sup> References to “Member States” made throughout this document should be understood as references to “EEA Member States”.

<sup>2</sup> Article 29 Working Party Opinion 1/2010 on the concepts of “controller” and “processor” adopted on 16 February 2010, 264/10/EN, WP 169.

to give more developed and specific guidance in order to ensure a consistent and harmonised approach throughout the EU and the EEA. The present guidelines replace the previous opinion of Working Party 29 on these concepts (WP169).

5. In part I, these guidelines discuss the definitions of the different concepts of controller, joint controllers, processor and third party/recipient. In part II, further guidance is provided on the consequences that are attached to the different roles of controller, joint controllers and processor.

## PART I – CONCEPTS

### 1 GENERAL OBSERVATIONS

6. The GDPR, in Article 5(2), explicitly introduces the accountability principle which means that:
  - the controller shall be *responsible for the compliance* with the principles set out in Article 5(1) GDPR; and that
  - the controller shall be able to *demonstrate compliance* with the principles set out in Article 5(1) GDPR.This principle has been described in an opinion by the Article 29 WP<sup>3</sup> and will not be discussed in detail here.
7. The aim of incorporating the accountability principle into the GDPR and making it a central principle was to emphasize that data controllers must implement appropriate and effective measures and be able to demonstrate compliance.<sup>4</sup>
8. The accountability principle has been further elaborated in Article 24, which states that the controller shall implement appropriate technical and organisational measures to ensure and to be able **to demonstrate** that processing is performed in accordance with the GDPR. Such measures shall be reviewed and updated if necessary. The accountability principle is also reflected in Article 28, which lays down the controller's obligations when engaging a processor.
9. The accountability principle is directly addressed to the controller. However, some of the more specific rules are addressed to both controllers and processors, such as the rules on supervisory authorities' powers in Article 58. Both controllers and processors can be fined in case of non-compliance with the obligations of the GDPR that are relevant to them and both are directly accountable towards supervisory authorities by virtue of the obligations to maintain and provide appropriate documentation upon request, co-operate in case of an investigation and abide by administrative orders. At the same time, it should be recalled that processors must always comply with, and act only on, instructions from the controller.
10. The accountability principle, together with the other, more specific rules on how to comply with the GDPR and the distribution of responsibility, therefore makes it necessary to define the different roles of several actors involved in a personal data processing activity.

---

<sup>3</sup> Article 29 Working Party Opinion 3/2010 on the principle of accountability adopted on 13 July 2010, 00062/10/EN WP 173.

<sup>4</sup> Recital 74 GDPR.

11. A general observation regarding the concepts of controller and processor in the GDPR is that they have not changed compared to the Directive 95/46/EC and that overall, the criteria for how to attribute the different roles remain the same.
12. The concepts of controller and processor are *functional* concepts: they aim to allocate responsibilities according to the actual roles of the parties.<sup>5</sup> This implies that the legal status of an actor as either a “controller” or a “processor” must in principle be determined by its actual activities in a specific situation, rather than upon the formal designation of an actor as being either a “controller” or “processor” (e.g. in a contract).<sup>6</sup> This means that the allocation of the roles usually should stem from an analysis of the factual elements or circumstances of the case and as such is not negotiable.
13. The concepts of controller and processor are also *autonomous* concepts in the sense that, although external legal sources can help identifying who is a controller, it should be interpreted mainly according to EU data protection law. The concept of controller should not be prejudiced by other - sometimes colliding or overlapping - concepts in other fields of law, such as the creator or the right holder in intellectual property rights or competition law.
14. As the underlying objective of attributing the role of controller is to ensure accountability and the effective and comprehensive protection of the personal data, the concept of ‘controller’ should be interpreted in a sufficiently broad way, favouring as much as possible effective and complete protection of data subjects<sup>7</sup> so as to ensure full effect of EU data protection law, to avoid lacunae and to prevent possible circumvention of the rules, while at the same time not diminishing the role of the processor.

## 2 DEFINITION OF CONTROLLER

### 2.1 Definition of controller

15. A controller is defined by Article 4(7) GDPR as

***“the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law”.***

16. The definition of controller contains five main building blocks, which will be analysed separately for the purposes of these Guidelines. They are the following:
  - “the natural or legal person, public authority, agency or other body”

---

<sup>5</sup> Article 29 Working Party Opinion 1/2010, WP 169, p. 9.

<sup>6</sup> See also the Opinion of Advocate General Mengozzi, in *Jehovah’s witnesses*, C-25/17, ECLI:EU:C:2018:57, paragraph 68 (“*For the purposes of determining the ‘controller’ within the meaning of Directive 95/46, I am inclined to consider [...] that excessive formalism would make it easy to circumvent the provisions of Directive 95/46 and that, consequently, it is necessary to rely upon a more factual than formal analysis [...].*”)

<sup>7</sup> CJEU, Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, judgment of 13 May 2014, paragraph 34; CJEU, Case C-210/16, Wirtschaftsakademie Schleswig-Holstein, judgment of 5 June 2018, paragraph 28; CJEU, Case C-40/17, Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV, judgment of 29 July 2019, paragraph 66.

- “determines”
- “alone or jointly with others”
- “the purposes and means”
- “of the processing of personal data”.

### **2.1.1 “Natural or legal person, public authority, agency or other body”**

17. The first building block relates to the type of entity that can be a controller. Under the GDPR, a controller can be “*a natural or legal person, public authority, agency or other body*”. This means that, in principle, there is no limitation as to the type of entity that may assume the role of a controller. It might be an organisation, but it might also be an individual or a group of individuals.<sup>8</sup> In practice, however, it is usually the organisation as such, and not an individual within the organisation (such as the CEO, an employee or a member of the board), that acts as a controller within the meaning of the GDPR. As far as data processing within a company group is concerned, special attention must be paid to the question of whether an establishment may be acting as a controller or processor, e.g. when processing data on behalf of the parent company.
18. Sometimes, companies and public bodies appoint a specific person responsible for the implementation of the processing activity. Even if a specific natural person is appointed to ensure compliance with data protection rules, this person will not be the controller but will act on behalf of the legal entity (company or public body) which will be ultimately responsible in case of infringement of the rules in its capacity as controller. In the same vein, even if a particular department or unit of an organisation has operational responsibility for ensuring compliance for certain processing activity, it does not mean that this department or unit (rather than the organisation as a whole) becomes the controller.

**Example:**

The marketing department of Company ABC launches an advertising campaign to promote ABC’s products. The marketing department decides the nature of campaign, the means to be used (e-mail, social media ...), which customers to target and what data to use in order to make the campaign as successful as possible. Even if the marketing department acted with considerable independence, Company ABC will in principle be considered as the controller seeing as the advertising campaign is launched by the company and takes place within the realm of its business activities and for its purposes.

19. In principle, any processing of personal data by employees which takes place within the realm of activities of an organisation may be presumed to take place under that organisation’s control.<sup>9</sup> In exceptional circumstances, however, it may occur that an employee decides to use personal data for his or her own purposes, thereby unlawfully exceeding the authority that he or she was given. (e.g. to set up his own company or similar). It is therefore the organisation’s duty as controller to make sure

---

<sup>8</sup> For example, in its Judgment in *Jehovah’s witnesses*, C-25/17, ECLI:EU:C:2018:551, paragraph 75, the CJEU considered that a religious community of Jehovah’s witnesses acted as a controller, jointly with its individual members. Judgment in *Jehovah’s witnesses*, C-25/17, ECLI:EU:C:2018:551, paragraph 75.

<sup>9</sup> Employees who have access to personal data within an organisation are generally not considered as “controllers” or “processors”, but rather as “persons acting under the authority of the controller or of the processor” within the meaning of article 29 GDPR.

that there are adequate technical and organizational measures, including e.g. training and information to employees, to ensure compliance with the GDPR.<sup>10</sup>

### 2.1.2 “Determines”

20. The second building block of the controller concept refers to the controller's *influence* over the processing, by virtue of an *exercise of decision-making power*. A controller is a body that *decides* certain key elements about the processing. This controllership may be defined by law or may stem from an analysis of the factual elements or circumstances of the case. One should look at the specific processing operations in question and understand who determines them, by first considering the following questions: "*why is this processing taking place?*" and "*who decided that the processing should take place for a particular purpose?*".

#### Circumstances giving rise to control

21. Having said that the concept of controller is a functional concept, it is therefore based on a **factual rather than a formal analysis**. In order to facilitate the analysis, certain rules of thumb and practical presumptions may be used to guide and simplify the process. In most situations, the "determining body" can be easily and clearly identified by reference to certain legal and/or factual circumstances from which "influence" normally can be inferred, unless other elements indicate the contrary. Two categories of situations can be distinguished: (1) control stemming from *legal provisions*; and (2) control stemming from *factual influence*.

##### 1) Control stemming from legal provisions

22. There are cases where control can be inferred from explicit legal competence e.g., when the controller or the specific criteria for its nomination are designated by national or Union law. Indeed, Article 4(7) states that "*where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.*" While Article 4(7) only refers to "the controller" in the singular form, the EDPB considers that it may also be possible for Union or Member State law to designate more than one controller, possibly even as joint controllers.
23. Where the controller has been specifically identified by law this will be determinative for establishing who is acting as controller. This presupposes that the legislator has designated as controller the entity that has a genuine ability to exercise control. In some countries, the national law provides that public authorities are responsible for processing of personal data within the context of their duties.
24. However, more commonly, rather than directly appointing the controller or setting out the criteria for its appointment, the law will establish a task or impose a duty on someone to collect and process certain data. In those cases, the purpose of the processing is often determined by the law. The controller will normally be the one designated by law for the realization of this purpose, this public task. For example, this would be the case where an entity which is entrusted with certain public tasks (e.g., social security) which cannot be fulfilled without collecting at least some personal data, sets up a database or register in order to fulfil those public tasks. In that case, the law, albeit indirectly, sets out who is the controller. More generally, the law may also impose an obligation on either public or private entities to retain or provide certain data. These entities would then normally be considered as controllers with respect to the processing that is necessary to execute this obligation.

---

<sup>10</sup> Article 24(1) GDPR.

**Example: Legal provisions**

The national law in Country A lays down an obligation for municipal authorities to provide social welfare benefits such as monthly payments to citizens depending on their financial situation. In order to carry out these payments, the municipal authority must collect and process data about the applicants' financial circumstances. Even though the law does not explicitly state that the municipal authorities are controllers for this processing, this follows implicitly from the legal provisions.

**2) Control stemming from factual influence**

25. In the absence of control arising from legal provisions, the qualification of a party as controller must be established on the basis of an assessment of the factual circumstances surrounding the processing. All relevant factual circumstances must be taken into account in order to reach a conclusion as to whether a particular entity exercises a determinative influence with respect to the processing of personal data in question.
26. The need for factual assessment also means that the role of a controller does not stem from the nature of an entity that is processing data but from its concrete activities in a specific context. In other words, the same entity may act at the same time as controller for certain processing operations and as processor for others, and the qualification as controller or processor has to be assessed with regard to each specific data processing activity.
27. In practice, certain processing activities can be considered as naturally attached to the role or activities of an entity ultimately entailing responsibilities from a data protection point of view. This can be due to more general legal provisions or an established legal practice in different areas (civil law, commercial law, labor law etc.). In this case, existing traditional roles and professional expertise that normally imply a certain responsibility will help in identifying the controller, for example: an employer in relation to processing personal data about his employees, a publisher processing personal data about its subscribers, or an association processing personal data about its members or contributors. When an entity engages in processing of personal data as part of its interactions with its own employees, customers or members, it will generally be the one who determines the purpose and means around the processing and is therefore acting as a controller within the meaning of the GDPR.

**Example: Law firms**

The company ABC hires a law firm to represent it in a dispute. In order to carry out this task, the law firm needs to process personal data related to the case. The reasons for processing the personal data is the law firm's mandate to represent the client in court. This mandate however is not specifically targeted to personal data processing. The law firm acts with a significant degree of independence, for example in deciding what information to use and how to use it, and there are no instructions from the client company regarding the personal data processing. The processing that the law firm carries out in order to fulfil the task as legal representative for the company is therefore linked to the functional role of the law firm so that it is to be regarded as controller for this processing.

**Example: Telecom operators<sup>11</sup>:**

---

<sup>11</sup> The EDPB considers that this example, previously included in Recital (47) of Directive 95/46/EC, remains relevant also under the GDPR.

Providing an electronic communications service such as an electronic mail service involves processing of personal data. The provider of such services will normally be considered a controller in respect of the processing of personal data that is necessary for the operation of the service as such (e.g., traffic and billing data). If the sole purpose and role of the provider is to enable the transmission of email messages, the provider will not be considered as the controller in respect of the personal data contained in the message itself. The controller in respect of any personal data contained inside the message will normally be considered to be the person from whom the message originates, rather than the service provider offering the transmission service.

28. In many cases, an assessment of the contractual terms between the different parties involved can facilitate the determination of which party (or parties) is acting as controller. Even if a contract is silent as to who is the controller, it may contain sufficient elements to infer who exercises a decision-making role with respect to the purposes and means of the processing. It may also be that the contract contains an explicit statement as to the identity of the controller. If there is no reason to doubt that this accurately reflects the reality, there is nothing against following the terms of the contract. However, the terms of a contract are not decisive in all circumstances, as this would simply allow parties to allocate responsibility as they see fit. It is not possible either to become a controller or to escape controller obligations simply by shaping the contract in a certain way where the factual circumstances say something else.
29. If one party in fact decides why and how personal data are processed that party will be a controller even if a contract says that it is a processor. Similarly, it is not because a commercial contract uses the term “subcontractor” that an entity shall be considered a processor from the perspective of data protection law.<sup>12</sup>
30. In line with the factual approach, the word “determines” means that the entity that actually exerts a decisive influence on the purposes and means of the processing is the controller. Normally, a processor agreement establishes who the determining party (controller) and the instructed party (processor) are. Even if the processor offers a service that is preliminary defined in a specific way, the controller has to be presented with a detailed description of the service and must make the final decision to actively approve the way the processing is carried out and request changes if necessary. Furthermore, the processor cannot at a later stage change the essential elements of the processing without the approval of the controller.

#### **Example: standardised cloud storage service**

A large cloud storage provider offers its customers the ability to store large volumes of personal data. The service is completely standardised, with customers having little or no ability to customise the service. The terms of the contract are determined and drawn up unilaterally by the cloud service provider, provided to the customer on a “take it or leave it basis”. Company X decides to make use of the cloud provider to store personal data concerning its customers. Company X will still be considered a controller, given its decision to make use of this particular cloud service provider in order to process personal data for its purposes. Insofar as the cloud service provider does not process the personal data for its own purposes and stores the data solely on behalf of its customers and in accordance with instructions, the service provider will be considered as a processor.

---

<sup>12</sup> See e.g., Article 29 Data Protection Working Party, Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), 22 November 2006, WP128, p. 11.

### 2.1.3 “Alone or jointly with others”

31. Article 4(7) recognizes that the “purposes and means” of the processing might be determined by more than one actor. It states that the controller is the actor who “alone or jointly with others” determines the purposes and means of the processing. This means that several different entities may act as controllers for the same processing, with each of them then being subject to the applicable data protection provisions. Correspondingly, an organisation can still be a controller even if it does not make all the decisions as to purposes and means. The criteria for joint controllership and the extent to which two or more actors jointly exercise control may take different forms, as clarified later on.<sup>13</sup>

### 2.1.4 “Purposes and means”

32. The fourth building block of the controller definition refers to the object of the controller’s influence, namely the “purposes and means” of the processing. It represents the substantive part of the controller concept: what a party should determine in order to qualify as controller.
33. Dictionaries define “purpose” as “an anticipated outcome that is intended or that guides your planned actions” and “means” as “how a result is obtained or an end is achieved”.
34. The GDPR establishes that data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Determination of the “purposes” of the processing and the “means” to achieve them is therefore particularly important.
35. Determining the purposes and the means amounts to deciding respectively the “why” and the “how” of the processing:<sup>14</sup> given a particular processing operation, the controller is the actor who has determined *why* the processing is taking place (i.e., “to what end”; or “what for”) and *how* this objective shall be reached (i.e. which means shall be employed to attain the objective). A natural or legal person who exerts such influence over the processing of personal data, thereby participates in the determination of the purposes and means of that processing in accordance with the definition in Article 4(7) GDPR.<sup>15</sup>
36. The controller must decide on both purpose and means of the processing as described below. As a result, the controller cannot settle with only determining the purpose. It must also make decisions about the means of the processing. Conversely, the party acting as processor can never determine the purpose of the processing.
37. In practice, if a controller engages a processor to carry out the processing on its behalf, it often means that the processor shall be able to make certain decisions of its own on how to carry out the processing. The EDPB recognizes that some margin of manoeuvre may exist for the processor also to be able to make some decisions in relation to the processing. In this perspective, there is a need to provide guidance about which **level of influence** on the “why” and the “how” should entail the qualification of an entity as a controller and to what extent a processor may make decisions of its own.
38. When one entity clearly determines purposes and means, entrusting another entity with processing activities that amount to the execution of its detailed instructions, the situation is straightforward, and there is no doubt that the second entity should be regarded as a processor, whereas the first entity is the controller.

---

<sup>13</sup> See Part I, Section 3 (“Definition of joint controllers”).

<sup>14</sup> See also the Opinion of Advocate General Bot in *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2017:796, paragraph 46.

<sup>15</sup> Judgment in *Jehovah’s witnesses*, C-25/17, ECLI:EU:C:2018:551, paragraph 68.

### Essential vs. non-essential means

39. The question is where to draw the line between decisions that are reserved to the controller and decisions that can be left to the discretion of the processor. Decisions on the purpose of the processing are clearly always for the controller to make.
40. As regards the determination of means, a distinction can be made between essential and non-essential means. “Essential means” are traditionally and inherently reserved to the controller. While non-essential means can also be determined by the processor, essential means are to be determined by the controller. “Essential means” are means that are closely linked to the purpose and the scope of the processing, such as the type of personal data which are processed (“*which data shall be processed?*”), the duration of the processing (“*for how long shall they be processed?*”), the categories of recipients (“*who shall have access to them?*”) and the categories of data subjects (“*whose personal data are being processed?*”). Together with the purpose of processing, the essential means are also closely linked to the question of whether the processing is lawful, necessary and proportionate. “Non-essential means” concern more practical aspects of implementation, such as the choice for a particular type of hard- or software or the detailed security measures which may be left to the processor to decide on.

#### **Example: Payroll administration**

Employer A hires another company to administer the payment of salaries to its employees. Employer A gives clear instructions on who to pay, what amounts, by what date, by which bank, how long the data shall be stored, what data should be disclosed to the tax authority etc. In this case, the processing of data is carried out for Company A’s purpose to pay salaries to its employees and the payroll administrator may not use the data for any purpose of its own. The way in which the payroll administrator should carry out the processing is in essence clearly and tightly defined. Nevertheless, the payroll administrator may decide on certain detailed matters around the processing such as which software to use, how to distribute access within its own organisation etc. This does not alter its role as processor as long as the administrator does not go against or beyond the instructions given by Company A.

#### **Example: Bank payments**

As part of the instructions from Employer A, the payroll administration transmits information to Bank B so that they can carry out the actual payment to the employees of Employer A. This activity includes processing of personal data by Bank B which it carries out for the purpose of performing banking activity. Within this activity, the bank decides independently from Employer A on which data that have to be processed to provide the service, for how long the data must be stored etc. Employer A cannot have any influence on the purpose and means of Bank B’s processing of data. Bank B is therefore to be seen as a controller for this processing and the transmission of personal data from the payroll administration is to be regarded as a disclosure of information between two controllers, from Employer A to Bank B.

#### **Example: Accountants**

Employer A also hires Accounting firm C to carry out audits of their bookkeeping and therefore transfers data about financial transactions (including personal data) to C. Accounting firm C processes these data without detailed instructions from A. Accounting firm C decides itself, in accordance with legal provisions regulating the tasks of the auditing activities carried out by C, that the data it collects

will only be processed for the purpose of auditing A and it determines what data it needs to have, which categories of persons that need to be registered, how long the data shall be kept and what technical means to use. Under these circumstances, Accounting firm C is to be regarded as a controller of its own when performing its auditing services for A. However, this assessment may be different depending on the level of instructions from A. In a situation where the law does not lay down specific obligations for the accounting firm and the client company provides very detailed instructions on the processing, the accounting firm would indeed be acting as a processor. A distinction could be made between a situation where the processing is - in accordance with the laws regulating this profession - done as part of the accounting firm's core activity and where the processing is a more limited, ancillary task that is carried out as part of the client company's activity.

#### **Example: Hosting services**

Employer A hires hosting service H to store encrypted data on H's servers. The hosting service H does not determine whether the data it hosts are personal data nor does it process data in any other way than storing it on its servers. As storage is one example of a personal data processing activity, the hosting service H is processing personal data on employer A's behalf and is therefore a processor. Employer A must provide the necessary instructions to H and a data processing agreement according to Article 28 must be concluded, requiring H to implement technical and organisational security measures. H must assist A in ensuring that the necessary security measures are taken and notify it in case of any personal data breach.

41. Even though decisions on non-essential means can be left to the processor, the controller must still stipulate certain elements in the processor agreement, such as – in relation to the security requirement, e.g. an instruction to take all measures required pursuant to Article 32 of the GDPR. The agreement must also state that the processor shall assist the controller in ensuring compliance with, for example, Article 32. In any event, the controller remains responsible for the implementation of appropriate technical and organisational measures to ensure and be able to demonstrate that the processing is performed in accordance with the Regulation (Article 24). In doing so, the controller must take into account the nature, scope, context and purposes of the processing as well as the risks for rights and freedoms of natural persons. For this reason, the controller must be fully informed about the means that are used so that it can take an informed decision in this regard. In order for the controller to be able to demonstrate the lawfulness of the processing, it is advisable to document at the minimum necessary technical and organisational measures in the contract or other legally binding instrument between the controller and the processor.

#### **Example: Call centre**

Company X decides to outsource a part of its customer service relations to a call centre. The call centre receives identifiable data about customer purchases, as well contact information. The call centre uses its own software and IT infrastructure to manage the personal data concerning Company X's customers. Company X signs a processor agreement with the provider of the call centre in accordance with Article 28 GDPR, after determining that the technical and organisational security measures proposed by the call centre are appropriate for the risks concerned and that the call centre will only process the personal data for the purposes of Company X and in accordance with its instructions. Company X does not provide any further instructions to the call centre as to specific software to be used nor any detailed instructions regarding the specific security measures to be implemented. In this example, Company X remains a controller, despite the fact that the call centre has determined certain non-essential means of the processing.

## 2.1.5 “Of the processing of personal data”

42. The purposes and means determined by the controller must relate to the “processing of personal data”. Article 4(2) GDPR defines the processing of personal data as “*any operation or set of operations which is performed on personal data or on sets of personal data*”. As a result, the concept of a controller can be linked either to a single processing operation or to a set of operations. In practice, this may mean that the control exercised by a particular entity may extend to the entirety of processing at issue but may also be limited to a particular stage in the processing.<sup>16</sup>
43. In practice, the processing of personal data involving several actors may be divided into several smaller processing operations for which each actor could be considered to determine the purpose and means individually. On the other hand, a sequence or set of processing operations involving several actors may also take place for the same purpose(s), in which case it is possible that the processing involves one or more joint controllers. In other words, it is possible that at “micro-level” the different processing operations of the chain appear as disconnected, as each of them may have a different purpose. However, it is necessary to double check whether at “macro-level” these processing operations should not be considered as a “set of operations” pursuing a joint purpose using jointly defined means.
44. Anyone who decides to process data must consider whether this includes personal data and, if so, what the obligations are according to the GDPR. An actor will be considered a “controller” even if it does not deliberately target personal data as such or has wrongfully assessed that it does not process personal data.
45. It is not necessary that the controller actually has access to the data that is being processed.<sup>17</sup> Someone who outsources a processing activity and in doing so, has a determinative influence on the purpose and (essential) means of the processing (e.g. by adjusting parameters of a service in such a way that it influences whose personal data shall be processed), is to be regarded as controller even though he or she will never have actual access to the data.

### Example: Market research 1

Company ABC wishes to understand which types of consumers are most likely to be interested in its products and contracts a service provider, XYZ, to obtain the relevant information.

Company ABC instructs XYZ on what type of information it is interested in and provides a list of questions to be asked to those participating in the market research.

Company ABC receives only statistical information (e.g., identifying consumer trends per region) from XYZ and does not have access to the personal data itself. Nevertheless, Company ABC decided that the processing should take place, the processing is carried out for its purpose and its activity and it has provided XYZ with detailed instructions on what information to collect. Company ABC is therefore still to be considered a controller with respect of the processing of personal data that takes place in order to deliver the information it has requested. XYZ may only process the data for the purpose given by Company ABC and according to its detailed instructions and is therefore to be regarded as processor.

<sup>16</sup> Judgment in *Fashion ID*, C-40/17, ECLI:EU:C:2019:629, paragraph 74: “(A)s the Advocate General noted, [...] it appears that a natural or legal person may be a controller, within the meaning of Article 2(d) of Directive 95/46, jointly with others only in respect of operations involving the processing of personal data for which it determines jointly the purposes and means. By contrast, [...] that natural or legal person cannot be considered to be a controller, within the meaning of that provision, in the context of operations that precede or are subsequent in the overall chain of processing for which that person does not determine either the purposes or the means”.

<sup>17</sup> Judgment in *Wirtschaftsakademie Schleswig-Holstein GmbH*, C-210/16, ECLI :EU :C :2018 :388, paragraph 38.

### **Example: Market research 2**

Company ABC wishes to understand which types of consumers are most likely to be interested in its products. Service provider XYZ is a market research agency which has collected information about consumer interests through a variety of questionnaires which pertain to a wide variety of products and services. Service provider XYZ has collected and analysed this data independently, according to its own methodology without receiving any instructions from Company ABC. To answer Company ABC's request, service provider XYZ will generate statistical information, but does so without receiving any further instructions about which personal data should be processed or how to process it in order to generate these statistics. In this example, service provider XYZ acts as the sole controller, processing personal data for market research purposes, autonomously determining the means for doing so. Company ABC does not have any particular role or responsibility under data protection law in relation to these processing activities, as Company ABC receives anonymised statistics and is not involved in determining the purposes and means of the processing.

## **3 DEFINITION OF JOINT CONTROLLERS**

### **3.1 Definition of joint controllers**

46. The qualification as joint controllers may arise where more than one actor is involved in the processing.
47. While the concept is not new and already existed under Directive 95/46/EC, the GDPR, in its Article 26, introduces specific rules for joint controllers and sets a framework to govern their relationship. In addition, the Court of Justice of the European Union (CJEU) in recent rulings has brought clarifications on this concept and its implications.<sup>18</sup>
48. As further elaborated in Part II, section 2, the qualification of joint controllers will mainly have consequences in terms of allocation of obligations for compliance with data protection rules and in particular with respect to the rights of individuals.
49. In this perspective, the following section aims to provide guidance on the concept of joint controllers in accordance with the GDPR and the CJEU case law to assist entities in determining where they may be acting as joint controllers and applying the concept in practice.

### **3.2 Existence of joint controllership**

#### **3.2.1 General considerations**

50. The definition of a controller in Article 4 (7) GDPR forms the starting point for determining joint controllership. The considerations in this section are thus directly related to and supplement the

---

<sup>18</sup> See in particular, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie*, (C-210/16), *Tietosuojavaltuutettu v Jehovan todistajat — uskonnollinen yhdyskunta* (C-25/17), *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV* (C-40/17). To be noted that while these judgments were issued by the CJEU on the interpretation of the concept of joint controllers under Directive 95/46/CE, they remain valid in the context of the GDPR, given that the elements determining this concept under the GDPR remain the same as under the Directive.

considerations in the section on the concept of controller. As a consequence, the assessment of joint controllership should mirror the assessment of "single" control developed above.

51. Article 26 GDPR, which reflects the definition in Article 4 (7) GDPR, provides that "[w]here two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers." In broad terms, joint controllership exists with regard to a specific processing activity when different parties determine *jointly* the purpose and means of this processing activity. Therefore, assessing the existence of joint controllers requires examining whether the determination of purposes and means that characterize a controller are decided by more than one party. "Jointly" must be interpreted as meaning "together with" or "not alone", in different forms and combinations, as explained below.
52. The assessment of joint controllership should be carried out on a factual, rather than a formal, analysis of the actual influence on the purposes and means of the processing. All existing or envisaged arrangements should be checked against the factual circumstances regarding the relationship between the parties. A merely formal criterion would not be sufficient for at least two reasons: in some cases, the formal appointment of a joint controller - laid down for example by law or in a contract - would be absent; in other cases, it may be that the formal appointment does not reflect the reality of the arrangements, by formally entrusting the role of controller to an entity which actually is not in the position to "determine" the purposes and means of the processing.
53. Not all processing involving several entities give rise to joint controllership. The overarching criterion for joint controllership to exist is the **joint participation of two or more entities in the determination of the purposes and means** of a processing. More specifically, joint participation needs to include the determination of purposes on the one hand and the determination of means on the other hand. If each of these elements are determined by all entities concerned, they should be considered as joint controllers of the processing at issue.

### 3.2.2 Assessment of joint participation

54. Joint participation in the determination of purposes and means implies that more than one entity have a decisive influence over whether and how the processing takes place. In practice, joint participation can take several different forms. For example, joint participation can take the form of a **common decision** taken by two or more entities or result from **converging decisions** by two or more entities regarding the purposes and essential means.
55. Joint participation through a *common decision* means deciding together and involves a common intention in accordance with the most common understanding of the term "jointly" referred to in Article 26 of the GDPR.

The situation of joint participation through *converging decisions* results more particularly from the case law of the CJEU on the concept of joint controllers. Decisions can be considered as converging on purposes and means if **they complement each other and are necessary for the processing to take place in such manner that they have a tangible impact on the determination of the purposes and means of the processing**. It should be highlighted that the notion of converging decisions needs to be considered in relation to the purposes and means of the processing but not other aspects of the commercial relationship between the parties.<sup>19</sup> As such, an important criterion to identify converging decisions in this context is **whether the processing would not be possible without both parties' participation in the purposes and means in the sense that the processing by each party is**

---

<sup>19</sup> Indeed, all commercial arrangements involve converging decisions as part of the process by which an agreement is reached.

**inseparable, i.e. inextricably linked.** The situation of joint controllers acting on the basis of converging decisions should however be distinguished from the case of a processor, since the latter – while participating in the performance of a processing – does not process the data for its own purposes but carries out the processing on behalf of the controller.

56. The fact that one of the parties does not have access to personal data processed is not sufficient to exclude joint controllership.<sup>20</sup> For example, in *Jehovah's Witnesses*, the CJEU considered that a religious community must be considered a controller, jointly with its members who engage in preaching, of the processing of personal data carried out by the latter in the context of door-to-door preaching.<sup>21</sup> The CJEU considered that it was not necessary that the community had access to the data in question, or to establish that that community had given its members written guidelines or instructions in relation to the data processing.<sup>22</sup> The community participated in the determination of purposes and means by organising and coordinating the activities of its members, which helped to achieve the objective of the Jehovah's Witnesses community.<sup>23</sup> In addition, the community had knowledge on a general level of the fact that such processing was carried out in order to spread its faith.<sup>24</sup>
57. It is also important to underline, as clarified by the CJEU, that an entity will be considered as joint controller with the other(s) only in respect of those operations for which it determines, jointly with others, the means and the purposes of the same data processing in particular in case of converging decisions. If one of these entities decides alone the purposes and means of operations that precede or are subsequent in the chain of processing, this entity must be considered as the sole controller of this preceding or subsequent operation.<sup>25</sup>
58. The existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data. On the contrary, the CJEU has clarified that those operators may be involved at different stages of that processing and to different degrees so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case.

### *3.2.2.1 Jointly determined purpose(s)*

59. Joint controllership exists when entities involved in the same processing carry out the processing for jointly defined purposes. This will be the case if the entities involved process the data for the same, or common, purposes.
60. In addition, when the entities do not have the same purpose for the processing, joint controllership may also, in light of the CJEU case law, be established when the entities involved pursue purposes which are closely linked or complementary. Such may be the case, for example, when there is a mutual benefit arising from the same processing operation, provided that each of the entities involved participates in the determination of the purposes and means of the relevant processing operation. However, the notion of mutual benefit is not decisive and can only be an indication.. In *Fashion ID*, for example, the CJEU clarified that a website operator participates in the determination of the purposes

---

<sup>20</sup> Judgment in *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, paragraph 38.

<sup>21</sup> Judgment in *Jehovah's witnesses*, C-25/17, ECLI:EU:C:2018:551, paragraph 75.

<sup>22</sup> Ibid.

<sup>23</sup> Ibid, paragraph 71.

<sup>24</sup> Ibid.

<sup>25</sup> Judgment in *Fashion ID*, C-40/17, ECLI:EU:2018:1039, paragraph 74 “*By contrast, and without prejudice to any civil liability provided for in national law in this respect, that natural or legal person cannot be considered to be a controller, within the meaning of that provision, in the context of operations that precede or are subsequent in the overall chain of processing for which that person does not determine either the purposes or the means*”.

(and means) of the processing by embedding a social plug-in on a website in order to optimize the publicity of its goods by making them more visible on the social network. The CJEU considered that the processing operations at issue were performed in the economic interests of both the website operator and the provider of the social plug-in.<sup>26</sup>

61. Likewise, as noted by the CJEU in *Wirtschaftsakademie*, the processing of personal data through statistics of visitors to a fan page is intended to enable Facebook to improve its system of advertising transmitted via its network and to enable the administrator of the fan page to obtain statistics to manage the promotion of its activity.<sup>27</sup> Each entity in this case pursues its own interest but both parties participate in the determination of the purposes (and means) of the processing of personal data as regards the visitors to the fan page.<sup>28</sup>
62. In this respect, it is important to highlight that the mere existence of a mutual benefit (for ex. commercial) arising from a processing activity does not give rise to joint controllership. If the entity involved in the processing does not pursue any purpose(s) of its own in relation to the processing activity, but is merely being paid for services rendered, it is acting as a processor rather than as a joint controller.

### *3.2.2.2 Jointly determined means*

63. Joint controllership also requires that two or more entities have exerted influence over the means of the processing. This does not mean that, for joint controllership to exist, each entity involved needs in all cases to determine all of the means. Indeed, as clarified by the CJEU, different entities may be involved at different stages of that processing and to different degrees. Different joint controllers may therefore define the means of the processing to a different extent, depending on who is effectively in a position to do so.
64. It may also be the case that one of the entities involved provides the means of the processing and makes it available for personal data processing activities by other entities. The entity who decides to make use of those means so that personal data can be processed for a particular purpose also participates in the determination of the means of the processing.
65. This scenario can notably arise in case of platforms, standardised tools, or other infrastructure allowing the parties to process the same personal data and which have been set up in a certain way by one of the parties to be used by others that can also decide how to set it up.<sup>29</sup> The use of an already existing technical system does not exclude joint controllership when users of the system can decide on the processing of personal data to be performed in this context.
66. As an example of this, the CJEU held in *Wirtschaftsakademie* that the administrator of a fan page hosted on Facebook, by defining parameters based on its target audience and the objectives of managing and promoting its activities, must be regarded as taking part in the determination of the means of the processing of personal data related to the visitors of its fan page.
67. Furthermore, the choice made by an entity to use for its own purposes a tool or other system developed by another entity, allowing the processing of personal data, will likely amount to a joint decision on the means of that processing by those entities. This follows from the *Fashion ID* case where

---

<sup>26</sup> Judgment in *Fashion ID*, C-40/17, ECLI:EU:2018:1039, paragraph 80.

<sup>27</sup> Judgment in *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, paragraph 34.

<sup>28</sup> Judgment in *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, paragraph 39.

<sup>29</sup> The provider of the system can be a joint controller if the criteria mentioned above are met, i.e. if the provider participates in the determination of purposes and means. Otherwise, the provider should be considered as a processor.

the CJEU concluded, that by embedding on its website the Facebook Like button made available by Facebook to website operators, Fashion ID has exerted a decisive influence in respect of the operations involving the collection and transmission of the personal data of the visitors of its website to Facebook and had thus jointly determined with Facebook the means of that processing.<sup>30</sup>

68. It is important to underline that **the use of a common data processing system or infrastructure will not in all cases lead to qualify the parties involved as joint controllers**, in particular where the processing they carry out is separable and could be performed by one party without intervention from the other or where the provider is a processor in the absence of any purpose of its own (the existence of a mere commercial benefit for the parties involved is not sufficient to qualify as a purpose of processing).

#### **Example: Travel agency**

A travel agency sends personal data of its customers to the airline and a chain of hotels, with a view to making reservations for a travel package. The airline and the hotel confirm the availability of the seats and rooms requested. The travel agency issues the travel documents and vouchers for its customers. Each of the actors processes the data for carrying out their own activities and using their own means. In this case, the travel agency, the airline and the hotel are three different data controllers processing the data for their own and separate purposes and there is no joint controllership.

The travel agency, the hotel chain and the airline then decide to participate jointly in setting up an internet-based common platform for the common purpose of providing package travel deals. They agree on the essential means to be used, such as which data will be stored, how reservations will be allocated and confirmed, and who can have access to the information stored. Furthermore, they decide to share the data of their customers in order to carry out joint marketing actions. In this case, the travel agency, the airline and the hotel chain, jointly determine why and how personal data of their respective customers are processed and will therefore be joint controllers with regard to the processing operations relating to the common internet-based booking platform and the joint marketing actions. However, each of them would still retain sole control with regard to other processing activities outside the internet-based common platform.

#### **Example: Research project by institutes**

Several research institutes decide to participate in a specific joint research project and to use to that end the existing platform of one of the institutes involved in the project. Each institute feeds personal data it already holds into the platform for the purpose of the joint research and uses the data provided by others through the platform for carrying out the research. In this case, all institutes qualify as joint controllers for the personal data processing that is done by storing and disclosing information from this platform since they have decided together the purpose of the processing and the means to be used (the existing platform). Each of the institutes however is a separate controller for any other processing that may be carried out outside the platform for their respective purposes.

#### **Example: Marketing operation**

Companies A and B have launched a co-branded product C and wish to organise an event to promote this product. To that end, they decide to share data from their respective clients and prospects

<sup>30</sup> Judgment in Fashion ID, C-40/17, ECLI:EU:2018:1039, paragraphs 77-79.

database and decide on the list of invitees to the event on this basis. They also agree on the modalities for sending the invitations to the event, how to collect feedback during the event and follow-up marketing actions. Companies A and B can be considered as joint controllers for the processing of personal data related to the organisation of the promotional event as they decide together on the jointly defined purpose and essential means of the data processing in this context.

#### **Example: Clinical Trials<sup>31</sup>**

A health care provider (the investigator) and a university (the sponsor) decide to launch together a clinical trial with the same purpose. They collaborate together to the drafting of the study protocol (i.e. purpose, methodology/design of the study, data to be collected, subject exclusion/inclusion criteria, database reuse (where relevant) etc.). They may be considered as joint controllers, for this clinical trial as they jointly determine and agree on the same purpose and the essential means of the processing. The collection of personal data from the medical record of the patient for the purpose of research is to be distinguished from the storage and use of the same data for the purpose of patient care, for which the health care provider remains the controller.

In the event that the investigator does not participate to the drafting of the protocol (he just accepts the protocol already elaborated by the sponsor), and the protocol is only designed by the sponsor, the investigator should be considered as a processor and the sponsor as the controller for this clinical trial.

#### **Example: Headhunters**

Company X helps Company Y in recruiting new staff- with its famous value-added service "global matchz". Company X looks for suitable candidates both among the CVs received directly by Company Y and those it already has in its own database. Such database is created and managed by Company X on its own. This ensures that Company X enhances the matching between job offers and job seekers, thus increasing its revenues. Even though they have not formally taken a decision together, Companies X and Y jointly participate to the processing with the purpose of finding suitable candidates based on converging decisions: the decision to create and manage the service "global matchz" for Company X and the decision of Company Y to enrich the database with the CVs it directly receives. Such decisions complement each other, are inseparable and necessary for the processing of finding suitable candidates to take place. Therefore, in this particular case they should be considered as joint controllers of such processing. However, Company X is the sole controller of the processing necessary to manage its database and Company Y is the sole controller of the subsequent hiring processing for its own purpose (organisation of interviews, conclusion of the contract and management of HR data).

#### **Example: Analysis of health data**

Company ABC, the developer of a blood pressure monitoring app and Company XYZ, a provider of apps for medical professionals, both wish to examine how blood pressure changes can help predict certain diseases. The companies decide to set up a joint project and reach out to Hospital DEF to become involved as well.

The personal data that will be processed in this project consists of personal data which Company ABC, Hospital DEF and Company XYZ are separately processing as individual controllers. The decision to

---

<sup>31</sup> The EDPB plans to provide further guidance in relation to clinical trials in the context of its forthcoming Guidelines on processing of personal data for medical and scientific research purposes.

process this data to assess blood pressure changes is taken jointly by the three actors. Company ABC, Hospital DEF and Company XYZ have jointly determined the purposes of processing. Company XYZ takes the initiative to propose the essential means of processing. Both Company ABC and the Hospital DEF accept these essential means after they as well were involved in developing some of the features of the app so that the results can be sufficiently used by them. The three organizations thus agree on having a common purpose for the processing which is the assessment of how blood pressure changes can help predict certain diseases. Once the research is completed, Company ABC, Hospital DEF and Company XYZ may benefit from the assessment by using its results in their own activities. For all these reasons, they qualify as joint controllers for this specific joint processing.

If Company XYZ had been simply asked by the others to perform this assessment without having any purpose of their own and merely been processing data on behalf of the others, Company XYZ would qualify as a processor even if it was entrusted with the determination of the non-essential means.

### 3.2.3 Situations where there is no joint controllership

69. The fact that several actors are involved in the same processing does not mean that they are necessarily acting as joint controllers of such processing. Not all kind of partnerships, cooperation or collaboration imply qualification of joint controllers as such qualification requires a case-by-case analysis of each processing at stake and the precise role of each entity with respect to each processing. The cases below provide non-exhaustive examples of situations where there is no joint controllership.
70. For example, the exchange of the same data or set of data between two entities without jointly determined purposes or jointly determined means of processing should be considered as a transmission of data between separate controllers.

#### **Example: Transmission of employee data to tax authorities**

A company collects and processes personal data of its employees with the purpose of managing salaries, health insurances, etc. A law imposes an obligation on the company to send all data concerning salaries to the tax authorities, with a view to reinforce fiscal control.

In this case, even though both the company and the tax authorities process the same data concerning salaries, the lack of jointly determined purposes and means with regard to this data processing will result in qualifying the two entities as two separate data controllers.

71. Joint controllership may also be excluded in a situation where several entities use a shared database or a common infrastructure, if each entity independently determines its own purposes.

#### **Example: Marketing operations in a group of companies using a shared database:**

A group of companies uses the same database for the management of clients and prospects. Such database is hosted on the servers of the mother company who is therefore a processor of the companies with respect to the storage of the data. Each entity of the group enters the data of its own clients and prospects and processes such data for its own purposes only. Also, each entity decides independently on the access, the retention periods, the correction or deletion of their clients and prospects' data. They cannot access or use each other's data. The mere fact that these companies use a shared group database does not as such entail joint controllership. Under these circumstances, each company is thus a separate controller.

#### **Example: Independent controllers when using a shared infrastructure**

Company XYZ hosts a database and makes it available to other companies to process and host personal data about their employees. Company XYZ is a processor in relation to the processing and storage of other companies' employees as these operations are performed on behalf and according to the instructions of these other companies. In addition, the other companies process the data without any involvement from Company XYZ and for purposes which are not in any way shared by Company XYZ.

72. Also, there can be situations where various actors successively process the same personal data in a chain of operations, each of these actors having an independent purpose and independent means in their part of the chain. In the absence of joint participation in the determination of the purposes and means of the same processing operation or set of operations, joint controllership has to be excluded and the various actors must be regarded as successive independent controllers.

**Example: Statistical analysis for a task of public interest**

A public authority (Authority A) has the legal task of making relevant analysis and statistics on how the country's employment rate develops. To do that, many other public entities are legally bound to disclose specific data to Authority A. Authority A decides to use a specific system to process the data, including collection. This also means that the other units are obligated to use the system for their disclosure of data. In this case, without prejudice to any attribution of roles by law, Authority A will be the only controller of the processing for the purpose of analysis and statistics of the employment rate processed in the system, because Authority A determines the purpose for the processing, and has decided how the processing will be organised. Of course, the other public entities, as controllers for their own processing activities, are responsible for ensuring the accuracy of the data they previously processed, which they then disclose to Authority A.

## 4 DEFINITION OF PROCESSOR

73. A processor is defined in Article 4 (8) as a natural or legal person, public authority, agency or another body, which processes personal data on behalf of the controller. Similar to the definition of controller, the definition of processor envisages a broad range of actors - it can be "*a natural or legal person, public authority, agency or other body*". This means that there is in principle no limitation as to which type of actor might assume the role of a processor. It might be an organisation, but it might also be an individual.
74. The GDPR lays down obligations directly applicable specifically to processors as further specified in Part II section 1 of these guidelines. A processor can be held liable or fined in case of failure to comply with such obligations or in case it acts outside or contrary to the lawful instructions of the controller.
75. Processing of personal data can involve multiple processors. For example, a controller may itself choose to directly engage multiple processors, by involving different processors at separate stages of the processing (multiple processors). A controller might also decide to engage one processor, who in turn - with the authorisation of the controller - engages one or more other processors ("sub processor(s)"). The processing activity entrusted to the processor may be limited to a very specific task or context or may be more general and extended.
76. Two basic conditions for qualifying as processor are:
- a) being *a separate entity* in relation to the controller and
  - b) processing personal data *on the controller's behalf*.

77. A *separate entity* means that the controller decides to delegate all or part of the processing activities to an external organisation. Within a group of companies, one company can be a processor to another company acting as controller, as both companies are separate entities. On the other hand, a department within a company cannot be a processor to another department within the same entity.
78. If the controller decides to process data itself, using its own resources within its organisation, for example through its own staff, this is not a processor situation. Employees and other persons that are acting under the direct authority of the controller, such as temporarily employed staff, are not to be seen as processors since they will process personal data as a part of the controller's entity. In accordance with Article 29, they are also bound by the controller's instructions.
79. *Processing personal data on the controller's behalf* firstly requires that the separate entity processes personal data for the benefit of the controller. In Article 4(2), processing is defined as a concept including a wide array of operations ranging from collection, storage and consultation to use, dissemination or otherwise making available and destruction.. The concept of "processing" is further described above under 2.1.5.
80. Secondly, the processing must be done on behalf of a controller but otherwise than under its direct authority or control. Acting "on behalf of" means serving someone else's interest and recalls the legal concept of "delegation". In the case of data protection law, a processor is called to implement the instructions given by the controller at least with regard to the purpose of the processing and the essential elements of the means. The lawfulness of the processing according to Article 6, and if relevant Article 9, of the Regulation will be derived from the controller's activity and the processor must not process the data otherwise than according to the controller's instructions. Even so, as described above, the controller's instructions may still leave a certain degree of discretion about how to best serve the controller's interests, allowing the processor to choose the most suitable technical and organisational means.<sup>32</sup>
81. Acting "on behalf of" also means that the processor may not carry out processing for its own purpose(s). As provided in Article 28(10), a processor infringes the GDPR by going beyond the controller's instructions and starting to determine its own purposes and means of processing. The processor will be considered a controller in respect of that processing and may be subject to sanctions for going beyond the controller's instructions.

**Example: Service provider referred to as data processor but acting as controller**

Service provider MarketinZ provides promotional advertisement and direct marketing services to various companies. Company GoodProductZ concludes a contract with MarketinZ, according to which the latter company provides commercial advertising for GoodProductZ customers and is referred to as data processor. However, MarketinZ decides to use GoodProducts customer database also for other purposes than advertising for GoodProducts, such as developing their own business activity. The decision to add an additional purpose to the one for which the personal data were transferred converts MarketinZ into a data controller for this set of processing operations and their processing for this purpose would constitute an infringement of the GDPR.

82. The EDPB recalls that not every service provider that processes personal data in the course of delivering a service is a "processor" within the meaning of the GDPR. The role of a processor does not stem from the nature of an entity that is processing data but from its concrete activities in a specific context. In other words, the same entity may act at the same time as a controller for certain processing

---

<sup>32</sup> See Part I, sub-section 2.1.4 describing the distinction between essential and non-essential means.

operations and as a processor for others, and the qualification as controller or processor has to be assessed with regard to specific sets of data or operations. The nature of the service will determine whether the processing activity amounts to processing of personal data on behalf of the controller within the meaning of the GDPR. In practice, where the provided service is not specifically targeted at processing personal data or where such processing does not constitute a key element of the service, the service provider may be in a position to independently determine the purposes and means of that processing which is required in order to provide the service. In that situation, the service provider is to be seen as a separate controller and not as a processor.<sup>33</sup> A case-by-case analysis remains necessary, however, in order to ascertain the degree of influence each entity effectively has in determining the purposes and means of the processing.

#### **Example: Taxi service**

A taxi service offers an online platform which allows companies to book a taxi to transport employees or guests to and from the airport. When booking a taxi, Company ABC specifies the name of the employee that should be picked up from the airport so the driver can confirm the employee's identity at the moment of pick-up. In this case, the taxi service processes personal data of the employee as part of its service to Company ABC, but the processing as such is not the target of the service. The taxi service has designed the online booking platform as part of developing its own business activity to provide transportation services, without any instructions from Company ABC. The taxi service also independently determines the categories of data it collects and how long it retains. The taxi service therefore acts as a controller in its own right, notwithstanding the fact that the processing takes place following a request for service from Company ABC.

83. The EDPB notes that a service provider may still be acting as a processor even if the processing of personal data is not the main or primary object of the service, provided that the customer of the service still determines the purposes and means of the processing in practice. When considering whether or not to entrust the processing of personal data to a particular service provider, controllers should carefully assess whether the service provider in question allows them to exercise a sufficient degree of control, taking into account the nature, scope, context and purposes of processing as well as the potential risks for data subjects.

#### **Example: Call center**

Company X outsources its client support to Company Y who provides a call center in order to help Company X's clients with their questions. The client support service means that Company Y has to have access to Company X client data bases. Company Y can only access data in order to provide the support that Company X has procured and they cannot process data for any other purposes than the ones stated by Company X. Company Y is to be seen as a personal data processor and a processor agreement must be concluded between Company X and Y.

#### **Example: General IT support**

Company Z hires an IT service provider to perform general support on its IT systems which include a vast amount of personal data. The access to personal data is not the main object of the support service but it is inevitable that the IT service provider systematically has access to personal data when

---

<sup>33</sup> See also Recital 81 of the GDPR, which refers to “entrusting a processor processing activities”, indicating that the processing activity as such is an important part of the decision of the controller to ask a processor to process personal data on its behalf.

performing the service. Company Z therefore concludes that the IT service provider - being a separate company and inevitably being required to process personal data even though this is not the main objective of the service – is to be regarded as a processor. A processor agreement is therefore concluded with the IT service provider.

#### **Example: IT-consultant fixing a software bug**

Company ABC hires an IT-specialist from another company to fix a bug in a software that is being used by the company. The IT-consultant is not hired to process personal data, and Company ABC determines that any access to personal data will be purely incidental and therefore very limited in practice. ABC therefore concludes that the IT-specialist is not a processor (nor a controller in its own right) and that Company ABC will take appropriate measures according to Article 32 of the GDPR in order to prevent the IT-consultant from processing personal data in an unauthorised manner.

84. As stated above, nothing prevents the processor from offering a preliminarily defined service but the controller must make the final decision to actively approve the way the processing is carried out, at least insofar as concerns the essential means of the processing. As stated above, a processor has a margin of manoeuvre as regards non-essential means, see above under sub-section 2.1.4.

#### **Example: Cloud service provider**

A municipality has decided to use a cloud service provider for handling information in its school and education services. The cloud service provides messaging services, videoconferences, storage of documents, calendar management, word processing etc. and will entail processing of personal data about school children and teachers. The cloud service provider has offered a standardized service that is offered worldwide. The municipality however must make sure that the agreement in place complies with Article 28(3) of the GDPR, that the personal data of which it is controller are processed for the municipality's purposes only. It must also make sure that their specific instructions on storage periods, deletion of data etc. are respected by the cloud service provider regardless of what is generally offered in the standardized service.

## **5 DEFINITION OF THIRD PARTY/RECIPIENT**

85. The Regulation not only defines the concepts of controller and processor but also the concepts of recipient and third party. As opposed to the concepts of controller and processor, the Regulation does not lay down specific obligations or responsibilities for recipients and third parties. These can be said to be relative concepts in the sense that they describe a relation to a controller or processor from a specific perspective, e.g. a controller or processor discloses data to a recipient. A recipient of personal data and a third party may well simultaneously be regarded as a controller or processor from other perspectives. For example, entities that are to be seen as recipients or third parties from one perspective, are controllers for the processing for which they determine the purpose and means.

#### **Third party**

86. Article 4(10) defines a “*third party*” as a natural or legal person, public authority, agency or body other than
- the data subject,
  - the controller,
  - the processor and

- persons who, under the direct authority of the controller or processor, are authorised to process personal data.
87. The definition generally corresponds to the previous definition of “*third party*” in Directive 95/46/EC.
88. Whereas the terms “*personal data*”, “*data subject*”, “*controller*” and “*processor*” are defined in the Regulation, the concept of “*persons who, under the direct authority of the controller or processor, are authorised to process personal data*” is not. It is, however, generally understood as referring to persons that belong to the legal entity of the controller or processor (an employee or a role highly comparable to that of employees, e.g. interim staff provided via a temporary employment agency) but only insofar as they are authorized to process personal data. An employee etc. who obtains access to data that he or she is not authorised to access and for other purposes than that of the employer does not fall within this category. Instead, this employee should be considered as a third party vis-à-vis the processing undertaken by the employer. Insofar as the employee processes personal data for his or her own purposes, distinct from those of his or her employer, he or she will then be considered a controller and take on all the resulting consequences and liabilities in terms of personal data processing.<sup>34</sup>
89. A third party thus refers to someone who, in the specific situation at hand, is not a data subject, a controller, a processor or an employee. For example, the controller may hire a processor and instruct it to transfer personal data to a third party. This third party will then be considered a controller in its own right for the processing that it carries out for its own purposes. It should be noted that, within a group of companies, a company other than the controller or the processor is a third party, even though it belongs to the same group as the company who acts as controller or processor.

#### **Example: Cleaning services**

Company A concludes a contract with a cleaning service company to clean its offices. The cleaners are not supposed to access or otherwise process personal data. Even though they may occasionally come across such data when moving around in the office, they can carry out their task without accessing data and they are contractually prohibited to access or otherwise process personal data that Company A keeps as controller. The cleaners are not employed by Company A nor are they seen as being under the direct authority of that company. There is no intention to engage the cleaning service company or its employees to process personal data on Company A’s behalf. The cleaning service company and its employees are therefore to be seen as a third party and the controller must make sure that there are adequate security measures to prevent that they have access to data and lay down a confidentiality duty in case they should accidentally come across personal data.

#### **Example: Company groups – parent company and subsidiaries**

Companies X and Y form part of the Group Z. Companies X and Y both process data about their respective employees for employee administration purposes. At one point, the parent company ZZ decides to request employee data from all subsidiaries in order to produce group wide statistics. When transferring data from companies X and Y to ZZ, the latter is to be regarded as a third party regardless of the fact that all companies are part of the same group. Company ZZ will be regarded as controller for its processing of the data for statistical purposes.

---

<sup>34</sup> The employer (as original controller) could nevertheless retain some responsibility in case the new processing occurred because of a lack of adequate security measures.

## **Recipient**

90. Article 4(9) defines a “*recipient*” as a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. Public authorities are however not to be seen as recipients when they receive personal data in the framework of a particular inquiry in accordance with Union or Member State law (e.g. tax and customs authorities, financial investigation units etc.)<sup>35</sup>
91. The definition generally corresponds to the previous definition of “*recipient*” in Directive 95/46/EC.
92. The definition covers anyone who receives personal data, whether they are a third party or not. For example, when a controller sends personal data to another entity, either a processor or a third party, this entity is a recipient. A third party recipient shall be considered a controller for any processing that it carries out for its own purpose(s) after it receives the data.

### **Example: Disclosure of data between companies**

The travel agency ExploreMore arranges travels on request from its individual customers. Within this service, they send the customers’ personal data to airlines, hotels and organisations of excursions in order for them to carry out their respective services. ExploreMore, the hotels, airlines and excursion providers are each to be seen as controllers for the processing that they carry out within their respective services. There is no controller-processor relation. However, the airlines, hotels and excursion providers are to be seen as recipients when receiving the personal data from ExploreMore.

## **PART II – CONSEQUENCES OF ATTRIBUTING DIFFERENT ROLES**

### **1 RELATIONSHIP BETWEEN CONTROLLER AND PROCESSOR**

93. A distinct new feature in the GDPR are the provisions that impose obligations directly upon processors. For example, a processor must ensure that persons authorised to process the personal data have committed themselves to confidentiality (Article 28(3)); a processor must maintain a record of all categories of processing activities (Article 30(2)) and must implement appropriate technical and organisational measures (Article 32). A processor must also designate a data protection officer under certain conditions (Article 37) and has a duty to notify the controller without undue delay after becoming aware of a personal data breach (Article 33(2)). Furthermore, the rules on transfers of data to third countries (Chapter V) apply to processors as well as controllers. In this regard, the EDPB considers that Article 28(3) GDPR, while mandating a specific content for the necessary contract between controller and processor, imposes direct obligations upon processors, including the duty to assist the controller in ensuring compliance.<sup>36</sup>

#### **1.1 Choice of the processor**

94. The controller has the **duty to use “only processors providing sufficient guarantees** to implement appropriate technical and organisational measures”, so that processing meets the requirements of the

---

<sup>35</sup> See also Recital 31 of the GDPR

<sup>36</sup> For instance, the processor should assist the controller, where necessary and upon request, in ensuring compliance with obligations relating to data protection impact assessments (Recital 95 GDPR). This needs to be reflected in the contract between the controller and the processor pursuant to Article 28(3)(f) GDPR.

GDPR - including for the security of processing - and ensures the protection of data subject rights.<sup>37</sup> The controller is therefore responsible for assessing the sufficiency of the guarantees provided by the processor and should be able to prove that it has taken all of the elements provided in the GDPR into serious consideration.

95. The guarantees “provided” by the processor are those that the processor is able to **demonstrate to the satisfaction of the controller**, as those are the only ones that can effectively be taken into account by the controller when assessing compliance with its obligations. Often this will require an exchange of relevant documentation (e.g. privacy policy, terms of service, record of processing activities, records management policy, information security policy, reports of external data protection audits, recognised international certifications, like ISO 27000 series).
96. The controller’s assessment of whether the guarantees are sufficient is a form of risk assessment, which will greatly depend on the type of processing entrusted to the processor and needs to be made on a case-by-case basis, taking into account the nature, scope, context and purposes of processing as well as the risks for the rights and freedoms of natural persons. As a consequence, the EDPB cannot provide an exhaustive list of the documents or actions that the processor needs to show or demonstrate in any given scenario, as this largely depends on the specific circumstances of the processing.
97. The following elements<sup>38</sup> should be taken into account by the controller in order to assess the sufficiency of the guarantees: the processor’s **expert knowledge** (e.g. technical expertise with regard to security measures and data breaches); the processor’s **reliability**; the processor’s **resources**. The reputation of the processor on the market may also be a relevant factor for controllers to consider.
98. Furthermore, the adherence to an approved code of conduct or certification mechanism can be used as an element by which sufficient guarantees can be demonstrated.<sup>39</sup> The processors are therefore advised to inform the controller as to this circumstance, as well as to any change in such adherence.
99. The obligation to use only processors “providing sufficient guarantees” contained in Article 28(1) GDPR is a continuous obligation. It does not end at the moment where the controller and processor conclude a contract or other legal act. Rather the controller should, at appropriate intervals, verify the processor’s guarantees, including through audits and inspections where appropriate.<sup>40</sup>

## 1.2 Form of the contract or other legal act

100. Any processing of personal data by a processor must be governed by a contract or other legal act under EU or Member State law between the controller and the processor, as required by Article 28(3) GDPR.
101. Such legal act must be **in writing, including in electronic form**.<sup>41</sup> Therefore, non-written agreements (regardless of how thorough or effective they are) cannot be considered sufficient to meet the requirements laid down by Article 28 GDPR. To avoid any difficulties in demonstrating that the contract or other legal act is actually in force, the EDPB recommends ensuring that the necessary signatures are included in the legal act, in line with applicable law (e.g. contract law).

---

<sup>37</sup> Article 28(1) and Recital 81 GDPR.

<sup>38</sup> Recital 81 GDPR.

<sup>39</sup> Article 28(5) and Recital 81 GDPR.

<sup>40</sup> See also Article 28(3)h GDPR.

<sup>41</sup> Article 28(9) GDPR.

102. Furthermore, the contract or the other legal act under Union or Member State law must be **binding on the processor** with regard to the controller, i.e. it must establish obligations on the processor that are binding as a matter of EU or Member State law. Also it must set out the obligations of the controller. In most cases, there will be a contract, but the Regulation also refers to “other legal act”, such as a national law (primary or secondary) or other legal instrument. If the legal act does not include all the minimum required content, it must be supplemented with a contract or another legal act that includes the missing elements.
103. Since the Regulation establishes a clear obligation to enter into a written contract, where no other relevant legal act is in force, the absence thereof is an infringement of the GDPR.<sup>42</sup> Both the controller and processor are responsible for ensuring that there is a contract or other legal act to govern the processing.<sup>43</sup> Subject to the provisions of Article 83 of the GDPR, the competent supervisory authority will be able to direct an administrative fine against both the controller and the processor, taking into account the circumstances of each individual case. Contracts that have been entered into before the date of application of the GDPR should have been updated in light of Article 28(3). The absence of such update, in order to bring a previously existing contract in line with the requirements of the GDPR, constitutes an infringement of Article 28(3).

A written contract pursuant to Article 28(3) GDPR may be embedded in a broader contract, such as a service level agreement. In order to facilitate the demonstration of compliance with the GDPR, the EDPB recommends that the elements of the contract that seek to give effect to Article 28 GDPR be clearly identified as such in one place (for example in an annex).

104. In order to comply with the duty to enter into a contract, **the controller and the processor may choose to negotiate their own contract** including all the compulsory elements **or to rely, in whole or in part, on standard contractual clauses in relation to obligations under Article 28.**<sup>44</sup>

---

<sup>42</sup> The presence (or absence) of a written arrangement, however, is not decisive for the existence of a controller-processor relationship. Where there is reason to believe that the contract does not correspond with reality in terms of actual control, on the basis of a factual analysis of the circumstances surrounding the relationship between the parties and the processing of personal data being carried out, the agreement may be set aside. Conversely, a controller-processor relationship might still be held to exist in absence of a written processing agreement. This would, however, imply a violation of Article 28(3) GDPR. Moreover, in certain circumstances, the absence of a clear definition of the relationship between the controller and the processor may raise the problem of the lack of legal basis on which every processing should be based, e.g. in respect of the communication of data between the controller and the alleged processor.

<sup>43</sup> Article 28(3) is not only applicable to controllers. In the situation where only the processor is subject to the territorial scope of the GDPR, the obligation shall only be directly applicable to the processor, see also EDPB Guidelines 3/2018 on the territorial scope of the GDPR, p. 12.

<sup>44</sup> Article 28(6) GDPR. The EDPB recalls that standard contractual clauses for the purposes of compliance with Article 28 GDPR are not the same as standard contractual clauses referred to in Article 46(2). While the former further stipulate and clarify how the provisions of Article 28(3) and (4) will be fulfilled, the latter provide appropriate safeguards in case of transfer of personal data to a third country or an international organisation in the absence of an adequacy decision pursuant to Article 45(3).

105. A set of standard contractual clauses (SCCs) may be, alternatively, adopted by the Commission<sup>45</sup> or adopted by a supervisory authority, in accordance with the consistency mechanism.<sup>46</sup> These clauses could be part of a certification granted to the controller or processor pursuant to Articles 42 or 43.<sup>47</sup>
106. The EDPB would like to clarify that there is no obligation for controllers and processors to enter into a contract based on SCCs, nor is it to be necessarily preferred over negotiating an individual contract. Both options are viable for the purposes of compliance with data protection law, depending on the specific circumstances, as long as they meet the Article 28(3) requirements.
107. If the parties wish to take advantage of standard contractual clauses, the data protection clauses of their agreement must be the same as those of the SCCs. The SCCs will often leave some blank spaces to be filled in or options to be selected by the parties. Also, as also mentioned above, the SCCs will generally be embedded in a larger agreement describing the object of the contract, its financial conditions, and other agreed clauses: it will be possible for the parties to add additional clauses (e.g. applicable law and jurisdiction) as long as they do not contradict, directly or indirectly, the SCCs<sup>48</sup> and they do not undermine the protection afforded by the GDPR and EU or Member State data protection laws.
108. Contracts between controllers and processors may sometimes be drafted unilaterally by one of the parties. Which party or parties that draft the contract may depend on several factors, including: the parties' position in the market and contractual power, their technical expertise, as well as access to legal services. For instance, some service providers tend to set up standard terms and conditions, which include data processing agreements.
109. An agreement between the controller and processor must comply with the requirements of Article 28 GDPR in order to ensure that the processor processes personal data in compliance with the GDPR. Any such agreement should take into account the specific responsibilities of controllers and processors. Although Article 28 provides a list of points which must be addressed in any contract governing the relationship between controllers and processors it leaves room for negotiations between the parties to such contracts. In some situations a controller or a processor may be in a weaker negotiation power to customize the data protection agreement. Reliance on the standard contractual clauses adopted pursuant to Article 28 (subparagraphs 7 and 8) may contribute to rebalancing the negotiating positions and to ensure that the contracts respect the GDPR.

<sup>45</sup> Article 28(7) GDPR. Article 28(7) GDPR. Article 28(7) GDPR. Article 28(7) GDPR. See the EDPB-EDPS Joint Opinion 1/2021 on standard contractual clauses between controllers and processors: [https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-12021-standard\\_en](https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-12021-standard_en).

<sup>46</sup> Article 28(8) GDPR. The Register for Decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism, including standard contractual clauses for the purposes of compliance with Art. 28 GDPR, can be accessed here: [https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions\\_en](https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions_en).

<sup>47</sup> Article 28(6) GDPR.

<sup>48</sup> The EDPB recalls that the same degree of flexibility is allowed when the parties choose to use SCCs as appropriate safeguard for transfers to third countries pursuant to Article 46(2)(c) or Article 46(2)(d) GDPR. Recital 109 GDPR clarifies that "*The possibility for the controller or processor to use standard data-protection clauses adopted by the Commission or by a supervisory authority should prevent controllers or processors neither from including the standard data-protection clauses in a wider contract, such as a contract between the processor and another processor, nor from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses [...] or prejudice the fundamental rights or freedoms of the data subjects. Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses*".

110. The fact that the contract and its detailed terms of business are prepared by the service provider rather than by the controller is not in itself problematic and is not in itself a sufficient basis to conclude that the service provider should be considered as a controller. Also, the imbalance in the contractual power of a small data controller with respect to big service providers should not be considered as a justification for the controller to accept clauses and terms of contracts which are not in compliance with data protection law, nor can it discharge the controller from its data protection obligations. The controller must evaluate the terms and in so far as it freely accepts them and makes use of the service, it has also accepted full responsibility for compliance with the GDPR. Any proposed modification, by a processor, of data processing agreements included in standard terms and conditions should be directly notified to and approved by the controller, bearing in mind the degree of leeway that the processor enjoys with respect to non-essential elements of the means (see paragraphs 40-41 above). The mere publication of these modifications on the processor's website is not compliant with Article 28.

### 1.3 Content of the contract or other legal act

111. Before focusing on each of the detailed requirements set out by the GDPR as to the content of the contract or other legal act, some general remarks are necessary.
112. While the elements laid down by Article 28 of the Regulation constitute its core content, the contract should be a way for the controller and the processor to further clarify how such core elements are going to be implemented with detailed instructions. Therefore, **the processing agreement should not merely restate the provisions of the GDPR**: rather, it should include more specific, concrete information as to how the requirements will be met and which level of security is required for the personal data processing that is the object of the processing agreement. Far from being a pro-forma exercise, the negotiation and stipulation of the contract are a chance to specify details regarding the processing.<sup>49</sup> Indeed, the "protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors [...] requires a clear allocation of the responsibilities" under the GDPR.<sup>50</sup>
113. At the same time, the contract should **take into account "the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject"**.<sup>51</sup> Generally speaking, the contract between the parties should be drafted in light of the specific data processing activity. For instance, there is no need to impose particularly stringent protections and procedures on a processor entrusted with a processing activity from which only minor risks arise: while each processor must comply with the requirements set out by the Regulation, the measures and procedures should be tailored to the specific situation. In any event, all elements of Article 28(3) must be covered by the contract. At the same time, the contract should include some elements that may help the processor in understanding the risks to the rights and freedoms of data subjects arising from the processing: because the activity is performed on behalf of the controller, often the controller has a deeper understanding of the risks that the processing entails since the controller is aware of the circumstances in which the processing is embedded.
114. Moving on to the **required content** of the contract or other legal act, EDPB interprets Article 28(3) in a way that it needs to set out:

---

<sup>49</sup> See also EDPB Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR), p. 5.

<sup>50</sup> Recital 79 GDPR.

<sup>51</sup> Recital 81 GDPR.

- the **subject-matter** of the processing (for instance, video surveillance recordings of people entering and leaving a high-security facility). While the subject matter of the processing is a broad concept, it needs to be formulated with enough specifications so that it is clear what the main object of the processing is;
  - the **duration**<sup>52</sup> of the processing: the exact period of time, or the criteria used to determine it, should be specified; for instance, reference could be made to the duration of the processing agreement;
  - the **nature** of the processing: the type of operations performed as part of the processing (for instance: “filming”, “recording”, “archiving of images”, ...) **and purpose** of the processing (for instance: detecting unlawful entry). This description should be as comprehensive as possible, depending on the specific processing activity, so as to allow external parties (e.g. supervisory authorities) to understand the content and the risks of the processing entrusted to the processor.
  - the **type of personal data**: this should be specified in the most detailed manner as possible (for instance: video images of individuals as they enter and leave the facility). It would not be adequate merely to specify that it is “personal data pursuant to Article 4(1) GDPR” or “special categories of personal data pursuant to Article 9”. In case of special categories of data, the contract or legal act should at least specify which types of data are concerned, for example, “information regarding health records”, or “information as to whether the data subject is a member of a trade union”;
  - the **categories of data subjects**: this, too, should be indicated in a quite specific way (for instance: “visitors”, “employees”, delivery services etc.);
  - the **obligations and rights of the controller**: the rights of the controller are further dealt with in the following sections (e.g. with respect to the right of the controller to perform inspections and audits). As regards the obligations of the controller, examples include the controller’s obligation to provide the processor with the data mentioned in the contract, to provide and document any instruction bearing on the processing of data by the processor, to ensure, before and throughout the processing, compliance with the obligations set out in the GDPR on the processor’s part, to supervise the processing, including by conducting audits and inspections with the processor.
115. While the GDPR lists elements that always need to be included in the agreement, other relevant information may need to be included, depending on the context and the risks of the processing as well as any additional applicable requirement.

### *1.3.1 The processor must only process data on documented instructions from the controller (Art. 28(3)(a) GDPR)*

116. The need to specify this obligation stems from the fact that the processor processes data on behalf of the controller. Controllers must provide its processors with instructions related to each processing activity. Such instructions can include permissible and unacceptable handling of personal data, more detailed procedures, ways of securing data, etc. The processor shall not go beyond what is instructed by the controller. It is however possible for the processor to suggest elements that, if accepted by the controller, become part of the instructions given.

---

<sup>52</sup> The duration of the processing is not necessarily equivalent to the duration of the agreement (there may be legal obligations to keep the data longer or shorter).

- 117. When a processor processes data outside or beyond the controller's instructions, and this amounts to a decision determining the purposes and means of processing, the processor will be in breach of its obligations and will even be considered a controller in respect of that processing in accordance with Article 28(10) (see sub-section 1.5 below<sup>53</sup>).
- 118. The instructions issued by the controller must be **documented**. For these purposes, it is recommended to include a procedure and a template for giving further instructions in an annex to the contract or other legal act. Alternatively, the instructions can be provided in any written form (e.g. e-mail), as well as in any other documented form as long as it is possible to keep records of such instructions. In any event, to avoid any difficulties in demonstrating that the controller's instructions have been duly documented, the EDPB recommends keeping such instructions together with the contract or other legal act.
- 119. The duty for the processor to refrain from any processing activity not based on the controller's instructions also applies to **transfers** of personal data to a third country or international organisation. The contract should specify the requirements for transfers to third countries or international organisations, taking into account the provisions of Chapter V of the GDPR.
- 120. The EDPB recommends that controller pay due attention to this specific point especially when the processor is going to delegate some processing activities to other processors, and when the processor has divisions or units located in third countries. If the instructions by the controller do not allow for transfers or disclosures to third countries, the processor will not be allowed to assign the processing to a sub-processor in a third country, nor will he be allowed to have the data processed in one of his non-EU divisions.
- 121. A processor may process data other than on documented instructions of the controller **when the processor is required to process and/or transfer personal data on the basis of EU law or Member State law to which the processor is subject**. This provision further reveals the importance of carefully negotiating and drafting data processing agreements, as, for example, legal advice may need to be sought by either party as to the existence of any such legal requirement. This needs to be done in a timely fashion, as the processor has an obligation to inform the controller of such requirement before starting the processing. Only when that same (EU or Member State) law forbids the processor to inform the controller on "important grounds of public interest", there is no such information obligation. In any case, any transfer or disclosure may only take place if authorised by Union law, including in accordance with Article 48 of the GDPR.

*1.3.2 The processor must ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality (Art. 28(3)(b) GDPR)*

- 122. The contract needs to state that the processor must ensure that anyone it allows to process the personal data is committed to confidentiality. This may occur either via a specific contractual agreement, or due to statutory obligations already in place.
- 123. The broad concept of "persons authorised to process the personal data" includes employees and temporary workers. Generally speaking, the processor should make the personal data available only to the employees who actually need them to perform tasks for which the processor was hired by the controller.

---

<sup>53</sup> See Part II, sub-section 1.5 ("Processor determining purposes and means of processing").

124. The commitment or obligation of confidentiality must be “appropriate”, i.e. it must effectively forbid the authorised person from disclosing any confidential information without authorisation, and it must be sufficiently broad so as to encompass all the personal data processed on behalf of the controller as well as the conditions under which the personal data are processed.

*1.3.3 The processor must take all the measures required pursuant to Article 32 (Art. 28(3)(c) GDPR)*

125. Article 32 requires the controller and the processor to implement appropriate technical and organisational security measures. While this obligation is already directly imposed on the processor whose processing operations fall within the scope of the GDPR, the duty to take all measures required pursuant to Article 32 still needs to be reflected in the contract concerning the processing activities entrusted by the controller.
126. As indicated earlier, the processing contract should not merely restate the provisions of the GDPR. The contract needs to include or reference information as to the security measures to be adopted, **an obligation on the processor to obtain the controller's approval before making changes**, and a regular review of the security measures so as to ensure their appropriateness with regard to risks, which may evolve over time. The degree of detail of the information as to the security measures to be included in the contract must be such as to enable the controller to assess the appropriateness of the measures pursuant to Article 32(1) GDPR. Moreover, the description is also necessary in order to enable the controller to comply with its accountability duty pursuant to Article 5(2) and Article 24 GDPR as regards the security measures imposed on the processor. A corresponding obligation of the processor to assist the controller and to make available all information necessary to demonstrate compliance can be inferred from Art. 28.3 (f) and (h) GDPR.
127. The level of instructions provided by the controller to the processor as to the measures to be implemented will depend on the specific circumstances. In some cases, the controller may provide a clear and detailed description of the security measures to be implemented. In other cases, the controller may describe the minimum security objectives to be achieved, while requesting the processor to propose implementation of specific security measures. In any event, the controller must provide the processor with a description of the processing activities and security objectives (based on the controller's risk assessment), as well as approve the measures proposed by the processor. This could be included in an annex to the contract. The controller exercises its decision-making power over the main features of the security measures, be it by explicitly listing the measures or by approving those proposed by the processor.

*1.3.4 The processor must respect the conditions referred to in Article 28(2) and 28(4) for engaging another processor (Art. 28(3)(d) GDPR).*

128. The agreement must specify that the processor may not engage another processor without the controller's prior written authorisation and whether this authorisation will be specific or general. In case of general authorisation, the processor has to inform the controller of any change of sub-processors under a written authorisation, and give the controller the opportunity to object. It is recommended that the contract set out the process for this. It should be noted that the processor's duty to inform the controller of any change of sub-processors implies that the processor actively

indicates or flags such changes toward the controller.<sup>54</sup> Also, where specific authorisation is required, the contract should set out the process for obtaining such authorisation.

129. When the processor engages another processor, a contract must be put in place between them, imposing the same data protection obligations as those imposed on the original processor or these obligations must be imposed by another legal act under Union or Member State law (see also below paragraph 160). This includes the obligation under Article 28(3)(h) to allow for and contribute to audits by the controller or another auditor mandated by the controller.<sup>55</sup> The processor is liable to the controller for the other processors' compliance with data protection obligations (for further details on the recommended content of the agreement see sub-section 1.6 below<sup>56</sup>).

*1.3.5 The processor must assist the controller for the fulfilment of its obligation to respond to requests for exercising the data subject's rights (Article 28(3) (e) GDPR).*

130. While ensuring that data subjects requests are dealt with is up to the controller, the contract must stipulate that the processor has an obligation to provide assistance "by appropriate technical and organisational measures, insofar as this is possible". The nature of this assistance may vary greatly "taking into account the nature of the processing" and depending on the type of activity entrusted to the processor. The details concerning the assistance to be provided by the processor should be included in the contract or in an annex thereto.
131. While the assistance may simply consist in promptly forwarding any request received and/or enabling the controller to directly extract and manage the relevant personal data, in some circumstances the processor will be given more specific, technical duties, especially when it is in the position of extracting and managing the personal data.
132. It is crucial to bear in mind that, although the practical management of individual requests can be outsourced to the processor, the controller bears the responsibility for complying with such requests. Therefore, the assessment as to whether requests by data subjects are admissible and/or the requirements set by the GDPR are met should be performed by the controller, either on a case-by-case basis or through clear instructions provided to the processor in the contract before the start of the processing. Also, the deadlines set out by Chapter III cannot be extended by the controller based on the fact that the necessary information must be provided by the processor.

*1.3.6 The processor must assist the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 (Art. 28(3)(f) GDPR).*

133. It is necessary for the contract to avoid merely restating these duties of assistance: **the agreement should contain details as to how the processor is asked to help the controller meet the listed obligations.** For example, procedures and template forms may be added in the annexes to the agreement, allowing the processor to provide the controller with all the necessary information.
134. The type and degree of assistance to be provided by the processor may vary widely "*taking into account the nature of processing and the information available to the processor*". The controller must

---

<sup>54</sup> In this regard it is, by contrast, e.g. not sufficient for the processor to merely provide the controller with a generalized access to a list of the sub-processors which might be updated from time to time, without pointing to each new sub-processor envisaged. In other words, the processor must actively inform the controller of any change to the list (i.e. in particular of each new envisaged sub-processor).

<sup>55</sup> See also EDPB Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR), 9 July 2019, at paragraph 44.

<sup>56</sup> See Part II, sub-section 1.6 ("Sub-processors").

adequately inform the processor as to the risk involved in the processing and as to any other circumstance that may help the processor meet its duty.

135. Moving on to the specific obligations, the processor has, first, a duty to assist the controller in meeting the obligation to adopt adequate technical and organisational measures to ensure security of processing.<sup>57</sup> While this may overlap, to some extent, with the requirement that the processor itself adopts adequate security measures, where the processing operations of the processor fall within the scope of the GDPR, they remain two distinct obligations, since one refers to the processor's own measures and the other refers to the controller's.
136. Secondly, the processor must assist the controller in meeting the obligation to notify personal data breaches to the supervisory authority and to data subjects. The processor must notify the controller whenever it discovers a personal data breach affecting the processor's or a sub-processor's facilities / IT systems and help the controller in obtaining the information that need to be stated in the report to the supervisory authority.<sup>58</sup> The GDPR requires that the controller notify a breach without undue delay in order to minimize the harm for individuals and to maximize the possibility to address the breach in an adequate manner. Thus, the processor's notification to the data controller should also take place without undue delay.<sup>59</sup> Depending on the specific features of the processing entrusted to the processor, it may be appropriate for the parties to include in the contract a specific timeframe (e.g. number of hours) by which the processor should notify the controller, as well as the point of contact for such notifications, the modality and the minimum content expected by the controller.<sup>60</sup> The contractual arrangement between the controller and the processor may also include an authorisation and a requirement for the processor to directly notify a data breach in accordance with Articles 33 and 34, but the legal responsibility for the notification remains with the controller.<sup>61</sup> If the processor does notify a data breach directly to the supervisory authority, and inform data subjects in accordance with Article 33 and 34, the processor must also inform the controller and provide the controller with copies of the notification and information to data subjects.
137. Furthermore, the processor must also assist the controller in carrying out data protection impact assessments when required, and in consulting the supervisory authority when the outcome reveals that there is a high risk that cannot be mitigated.
138. The duty of assistance does not consist in a shift of responsibility, as those obligations are imposed on the controller. For instance, although the data protection impact assessment can in practice be carried out by a processor, the controller remains accountable for the duty to carry out the assessment<sup>62</sup> and the processor is only required to assist the controller "where necessary and upon request."<sup>63</sup> As a result, the controller is the one that must take the initiative to perform the data protection impact assessment, not the processor.

---

<sup>57</sup> Article 32 GDPR.

<sup>58</sup> Article 33(3) GDPR.

<sup>59</sup> For more information, see the Guidelines on Personal data breach notification under Regulation 2016/679, WP250rev.01, 6 February 2018, p. 13-14.

<sup>60</sup> See also EDPB Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR), 9 July 2019, at paragraph 40.

<sup>61</sup> Guidelines on Personal data breach notification under Regulation 2016/679, WP250rev.01, 6 February 2018, p. 14.

<sup>62</sup> Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 rev.01, p. 14

<sup>63</sup> Recital 95 GDPR.

*1.3.7 On termination of the processing activities, the processor must, at the choice of the controller, delete or return all the personal data to the controller and delete existing copies (Art. 28(3)(g) GDPR).*

139. The contractual terms are meant to ensure that the personal data are subject to appropriate protection after the end of the “provision of services related to the processing”: it is therefore up to the controller to decide what the processor should do with regard to the personal data.
140. The controller can decide at the beginning whether personal data shall be deleted or returned by specifying it in the contract, through a written communication to be timely sent to the processor. The contract or other legal act should reflect the possibility for the data controller to change the choice made before the end of the provision of services related to the processing. The contract should specify the process for providing such instructions.
141. If the controller chooses that the personal data be deleted, the processor should ensure that the deletion is performed in a secure manner, also in order to comply with Article 32 GDPR. The processor should confirm to the controller that the deletion has been completed within an agreed timescale and in an agreed manner.
142. The processor must delete all existing copies of the data, unless EU or Member State law requires further storage. If the processor or controller is aware of any such legal requirement, it should inform the other party as soon as possible.

*1.3.8 The processor must make available to the controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller (Art. 28(3)(h) GDPR).*

143. The contract shall include details on how often and how the flow of information between the processor and the controller should take place so that the controller is fully informed as to the details of the processing that are relevant to demonstrate compliance with the obligations laid down in Article 28 GDPR. For instance, the relevant portions of the processor’s records of processing activities may be shared with the controller. The processor should provide all information on how the processing activity will be carried out on behalf of the controller. Such information should include information on the functioning of the systems used, security measures, how the data retention requirements are met, data location, transfers of data, who has access to data and who are the recipients of data, sub-processors used, etc.
144. Further details shall also be set out in the contract regarding the ability to carry out and the duty to contribute to inspections and audits by the controller or another auditor mandated by the controller.

The GDPR specifies the inspections and audits are carried out by the controller or by a third party mandated by the controller. The goal of such audit is ensuring that the controller has all information concerning the processing activity performed on its behalf and the guarantees provided by the processor. The processor may suggest the choice of a specific auditor, but the final decision has to be left to the controller according to Article 28(3)(h) of the GDPR.<sup>64</sup> Additionally, even where the

---

<sup>64</sup> See EDPB-EDPS Joint Opinion 1/2021 on standard contractual clauses between controllers and processors, paragraph 43.

inspection is performed by an auditor proposed by the processor, the controller retains the right to contest the scope, methodology and results of the inspection.<sup>65</sup>

The parties should cooperate in good faith and assess whether and when there is a need to perform audits on the processor's premises,, as well as which type of audit or inspection (remote / on-site / other way to gather the necessary information) would be needed and appropriate in the specific case also taking into account security concerns; the final choice on this is to be taken by the controller. Following the results of the inspection, the controller should be able to request the processor to take subsequent measures, e.g. to remedy shortcomings and gaps identified.<sup>66</sup> Likewise, specific procedures should be established regarding the processor's and the controller's inspection of sub-processors (see sub-section 1.6 below<sup>67</sup>).

145. The issue of the allocation of costs between a controller and a processor concerning audits is not covered by the GDPR and is subject to commercial considerations. However, Article 28 (3)(h) requires that the contract include an obligation for the processor to make available all information necessary to the controller and an obligation to allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller. This means in practice that parties should not insert in the contract clauses envisaging the payment of costs or fees that would be clearly disproportionate or excessive, thus having a dissuasive effect on one of the parties. Such clauses would indeed imply that the rights and obligations set out in Article 28(3)(h) would never be exercised in practice and would become purely theoretical whereas they form an integral part of the data protection safeguards envisaged under Article 28 GDPR.

#### 1.4 Instructions infringing data protection law

146. According to Article 28(3), the processor must immediately inform the controller if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions.
147. Indeed, the processor has a duty to comply with the controller's instructions, but it also has a general obligation to comply with the law. An instruction that infringes data protection law seems to cause a conflict between the aforementioned two obligations.
148. Once informed that one of its instructions may be in breach of data protection law, the controller will have to assess the situation and determine whether the instruction actually violates data protection law.
149. The EDPB recommends the parties to negotiate and agree in the contract the consequences of the notification of an infringing instruction sent by the processor and in case of inaction from the controller in this context. One example would be to insert a clause on the termination of the contract if the controller persists with an unlawful instruction. Another example would be 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<sup>68</sup>.

---

<sup>65</sup> See Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR), paragraph 43.

<sup>66</sup> See Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR), paragraph 43.

<sup>67</sup> See Part II, sub-section 1.6 ("Sub-processors").

<sup>68</sup> See EDPB-EDPS Joint Opinion 1/2021 on standard contractual clauses between controllers and processors, paragraph 39.

## 1.5 Processor determining purposes and means of processing

150. If the processor infringes the Regulation by determining the purposes and means of processing, it shall be considered as a controller in respect of that processing (Article 28(10) GDPR).

## 1.6 Sub-processors

151. Data processing activities are often carried out by a great number of actors, and the chains of subcontracting are becoming increasingly complex. The GDPR introduces specific obligations that are triggered when a (sub-)processor intends to engage another player, thereby adding another link to the chain, by entrusting to it activities requiring the processing of personal data. The analysis of whether the service provider acts as a sub-processor should be carried out in line with what described above on the concept of processor (see above paragraph 83).
152. Although the chain may be quite long, the controller retains its pivotal role in determining the purpose and means of processing. Article 28(2) GDPR stipulates that the processor shall not engage another processor without prior specific or general written authorisation of the controller (including in electronic form). In the case of general written authorisation, the processor must inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes. In both cases, the processor must obtain the controller's authorisation in writing before any personal data processing is entrusted to the sub-processor. 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.<sup>69</sup>
153. The prior written authorisation may be specific, i.e. referring to a specific sub-processor for a specific processing activity and at a specific time, or general. This should be specified in the contract or other legal act that governs the processing.
154. In cases where the controller decides to accept certain sub-processors at the time of the signature of the contract, a list of approved sub-processors should be included in the contract or an annex thereto. The list should then be kept up to date, in accordance with the general or specific authorisation given by the controller.
155. If the controller chooses to give its **specific authorisation**, it should specify in writing which sub-processor and what processing activity it refers to. Any subsequent change will need to be further authorised by the controller before it is put in place. If the processor's request for a specific authorisation is not answered to within the set timeframe, it should be held as denied. The controller should make its decision to grant or withhold authorisation taking into account its obligation to only use processors providing "sufficient guarantees" (see sub-section 1.1 above<sup>70</sup>).
156. Alternatively, the controller may provide its **general authorisation** to the use of sub-processors (in the contract, including a list with such sub-processors in an annex thereto), which should be supplemented with criteria to guide the processor's choice (e.g., guarantees in terms of technical and organisational

---

<sup>69</sup> 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.

<sup>70</sup> See Part II - sub-section 1.1 ("Choice of the processor").

measures, expert knowledge, reliability and resources).<sup>71</sup> In this scenario, the processor needs to inform the controller in due time of any intended addition or replacement of sub-processor(s) so as to provide the controller with the opportunity to object.

157. Therefore, the main difference between the specific authorisation and the general authorisation scenarios lies in the meaning given to the controller's silence: in the general authorisation situation, the controller's failure to object within the set timeframe can be interpreted as authorisation.
158. In both scenarios, the contract should include details as to the timeframe for the controller's approval or objection and as to how the parties intend to communicate regarding this topic (e.g. templates). Such timeframe needs to be reasonable in light of the type of processing, the complexity of the activities entrusted to the processor (and the sub-processors) and the relationship between the parties. In addition, the contract should include details as to the practical steps following the controller's objection (e.g. by specifying time frame within which the controller and processor should decide whether the processing shall be terminated).
159. Regardless of the criteria suggested by the controller to choose providers, the processor remains fully liable to the controller for the performance of the sub-processors' obligations (Article 28(4) GDPR). Therefore, the processor should ensure it proposes sub-processors providing sufficient guarantees.
160. Furthermore, when a processor intends to employ an (authorised) sub-processor, it must enter into a contract with it that imposes the same obligations as those imposed on the first processor by the controller or the obligations must be imposed by another legal act under EU or Member State law. The whole chain of processing activities needs to be regulated by written agreements. Imposing the "same" obligations should be construed in a functional rather than in a formal way: it is not necessary for the contract to include exactly the same words as those used in the contract between the controller and the processor, but it should ensure that the obligations in substance are the same. This also means that if the processor entrusts the sub-processor with a specific part of the processing, to which some of the obligations cannot apply, such obligations should not be included "by default" in the contract with the sub-processor, as this would only generate uncertainty. As an example, as to assistance with data breach related obligations, notification of a data breach by a sub-processor directly to the controller could be done if all three agree. However, in the case of such direct notification the processor should be informed and get a copy of the notification.

## 2 CONSEQUENCES OF JOINT CONTROLLERSHIP

### 2.1 Determining in a transparent manner the respective responsibilities of joint controllers for compliance with the obligations under the GDPR

161. Article 26(1) of the GDPR provides that joint controllers shall in a transparent manner determine and agree on their respective responsibilities for compliance with the obligations under the Regulation.
162. Joint controllers thus need to set "who does what" by deciding between themselves who will have to carry out which tasks in order to make sure that the processing complies with the applicable obligations under the GDPR in relation to the joint processing at stake. In other words, a distribution of responsibilities for compliance is to be made as resulting from the use of the term "*respective*" in

---

<sup>71</sup> This duty of the controller stems from the accountability principle in Article 24 and from the obligation to comply with provisions of Articles 28(1), 32 and Chapter V of the GDPR.

Article 26(1). This does not preclude the fact that EU or Member State law may already set out certain responsibilities of each joint controller. Where this is the case, the joint controller arrangement should also address any additional responsibilities necessary to ensure compliance with the GDPR that are not addressed by the legal provisions.<sup>72</sup>

163. The objective of these rules is to ensure that where multiple actors are involved, especially in complex data processing environments, responsibility for compliance with data protection rules is clearly allocated in order to avoid that the protection of personal data is reduced, or that a negative conflict of competence lead to loopholes whereby some obligations are not complied with by any of the parties involved in the processing. It should be made clear here that all responsibilities have to be allocated according to the factual circumstances in order to achieve an operative agreement. The EDPB observes that there are situations occurring in which the influence of one joint controller and its factual influence complicate the achievement of an agreement. However, those circumstances do not negate the joint controllership and cannot serve to exempt either party from its obligations under the GDPR.
164. More specifically, Article 26(1) specifies that the determination of their respective responsibilities (i.e. tasks) for compliance with the obligations under the GDPR is to be carried out by joint controllers "*in particular*" as regards the exercising of the rights of the data subject and the duties to provide information referred in Articles 13 and 14, unless and in so far as the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject.
165. It is clear from this provision that joint controllers need to define who respectively will be in charge of answering to requests when data subjects exercise their rights granted by the GDPR and of providing information to them as required by Articles 13 and 14 of the GDPR. This only refers to defining in their internal relationship which of the parties is obligated to respond to which data subjects' requests. . Regardless of any such arrangement, the data subject may contact either of the joint controllers in accordance with Article 26 (3) GDPR. However, the use of the terms "*in particular*" indicates that the obligations subject to the allocation of responsibilities for compliance by each party involved as referred in this provision are non-exhaustive. It follows that the distribution of the responsibilities for compliance among joint controllers is not limited to the topics referred in Article 26(1) but extends to other controller's obligations under the GDPR. Indeed, joint controllers need to ensure that the whole joint processing fully complies with the GDPR.
166. In this perspective, the compliance measures and related obligations joint controllers should consider when determining their respective responsibilities, in addition to those specifically referred in Article 26(1), include amongst others without limitation:
  - Implementation of general data protection principles (Article 5)
  - Legal basis of the processing<sup>73</sup> (Article 6)
  - Security measures (Article 32)

---

<sup>72</sup> "In any event, the joint controller arrangement should comprehensively address all of the responsibilities of the joint controllers, including those which may have already been set out in the relevant EU or Member State law and without prejudice to the obligation of joint controllers to make available the essence of the joint controller arrangement in accordance with Article 26(2) GDPR."

<sup>73</sup> Although the GDPR does not preclude joint controllers to use different legal basis for different processing operations they carry out, it is recommended to use, whenever possible, the same legal basis for a particular purpose.

- Notification of a personal data breach to the supervisory authority and to the data subject<sup>74</sup> (Articles 33 and 34)
  - Data Protection Impact Assessments (Articles 35 and 36)<sup>75</sup>
  - The use of a processor (Article 28)
  - Transfers of data to third countries (Chapter V)
  - Organisation of contact with data subjects and supervisory authorities
167. Other topics that could be considered depending on the processing at stake and the intention of the parties are for instance the limitations on the use of personal data for another purpose by one of the joint controllers. In this respect, both controllers always have a duty to ensure that they both have a legal basis for the processing. Sometimes, in the context of joint controllership, personal data are shared by one controller to another. As a matter of accountability, each controller has the duty to ensure that the data are not further processed in a manner that is incompatible with the purposes for which they were originally collected by the controller sharing the data.<sup>76</sup>
168. Joint controllers can have a certain degree of flexibility in distributing and allocating obligations among them as long as they ensure full compliance with the GDPR with respect of the given processing. The allocation should take into account factors such as, who is competent and in a position to effectively ensure data subject's rights as well as to comply with the relevant obligations under the GDPR. The EDPB recommends documenting the relevant factors and the internal analysis carried out in order to allocate the different obligations. This analysis is part of the documentation under the accountability principle.
169. The obligations do not need to be equally distributed among the joint controllers. In this respect, the CJEU has recently stated that "*the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data*".<sup>77</sup> However, there may be cases where not all of the obligations can be distributed and all joint controllers may need to comply with the same requirements arising from the GDPR, taking into account the nature and context of the joint processing. For instance, joint controllers using shared data processing tools or systems both need to ensure compliance with notably the purpose limitation principle and implement appropriate measures to ensure the security of personal data processed under the shared tools.

---

<sup>74</sup> Please also see EDPB guidelines on Personal data breach notification under Regulation 2016/679, WP250.rev.01 which provide that joint controllership will include "*determining which party will have responsibility for complying with the obligations under Articles 33 and 34. WP29 recommends that the contractual arrangements between joint controllers include provisions that determine which controller will take the lead on, or be responsible for, compliance with the GDPR's breach notification obligations*" (p.13).

<sup>75</sup> Please also see EDPB guidelines on DPIAs, WP248.rev01 which provide the following: "*When the processing operation involves joint controllers, they need to define their respective obligations precisely. Their DPIA should set out which party is responsible for the various measures designed to treat risks and to protect the rights and freedoms of the data subjects. Each data controller should express his needs and share useful information without either compromising secrets (e.g.: protection of trade secrets, intellectual property, confidential business information) or disclosing vulnerabilities*" (p.7).

<sup>76</sup> Each disclosure by a controller requires a lawful basis and assessment of compatibility, regardless of whether the recipient is a separate controller or a joint controller. In other words, the existence of a joint controller relationship does not automatically mean that the joint controller receiving the data can also lawfully process the data for additional purposes which are beyond the scope of joint control.

<sup>77</sup> Judgment in *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, paragraph 43.

170. Another example is the requirement for each joint controller to maintain a record of processing activities or to designate a Data Protection Officer (DPO) if the conditions of Article 37(1) are met. Such requirements are not related to the joint processing but are applicable to them as controllers.

## 2.2 Allocation of responsibilities needs to be done by way of an arrangement

### 2.2.1 Form of the arrangement

171. Article 26(1) of the GDPR provides as a new obligation for joint controllers that they should determine their respective responsibilities “*by means of an arrangement between them*”. The legal form of such arrangement is not specified by the GDPR. Therefore, joint controllers are free to agree on the form of the arrangement.
172. In addition, the arrangement on the allocation of responsibilities is binding upon each of the joint controllers. They each agree and commit *vis-à-vis* each other on being responsible for complying with the respective obligations stated in their arrangement as their responsibility.
173. Therefore, for the sake of legal certainty, even if there is no legal requirement in the GDPR for a contract or other legal act, the EDPB recommends that such arrangement be made in the form of a binding document such as a contract or other legal binding act under EU or Member State law to which the controllers are subject. This would provide certainty and could be used to evidence transparency and accountability. Indeed, in case of non-compliance with the agreed allocation provided in the arrangement, its binding nature allows one controller to seek the liability of the other for what was stated in the agreement as falling under its responsibility. Also, in line with the accountability principle, the use of a contract or other legal act will allow joint controllers to demonstrate that they comply with the obligations imposed upon them by the GDPR.
174. The way responsibilities, i.e. the tasks, are allocated between each joint controller has to be stated in a clear and plain language in the arrangement.<sup>78</sup> This requirement is important as it ensures legal certainty and avoid possible conflicts not only in the relation between the joint controllers but also *vis-à-vis* the data subjects and the data protection authorities.
175. To better frame the allocation of responsibilities between the parties, the EDPB recommends that the arrangement also provide general information on the joint processing by notably specifying the subject matter and purpose of the processing, the type of personal data, and the categories of data subjects.

### 2.2.2 Obligations towards data subjects

176. The GDPR provides several obligations of joint controllers towards data subjects:

*The arrangement shall duly reflect the respective roles and relationships of the joint controllers *vis-à-vis* the data subjects*

177. As a complement to what is explained above in section 2.1 of the present guidelines, it is important that the joint controllers clarify in the arrangement their respective role, “*in particular*” as regards the exercise of the rights of the data subject and their duties to provide the information referred to in Articles 13 and 14. Article 26 of the GDPR stresses the importance of these specific obligations. The joint controllers must therefore organise and agree on how and by whom the information will be

---

<sup>78</sup> As stated in Recital 79 of the GDPR “*(...) the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear allocation of the responsibilities under this Regulation, including where a controller determines the purposes and means of the processing jointly with other controllers*”.

provided and how and by whom the answers to the data subject's requests will be provided. Irrespective of the content of the arrangement on this specific point, the data subject may contact either of the joint controllers to exercise his or her rights in accordance with Article 26(3) as further explained below.

178. The way these obligations are organised in the arrangement should "duly", i.e. accurately, reflect the reality of the underlying joint processing. For example, if only one of the joint controllers communicates with the data subjects for the purpose of the joint processing, such controller could be in a better position to inform the data subjects and possibly to answer their requests.

#### **The essence of the arrangement shall be made available to the data subject**

179. This provision is aimed to ensure that the data subject is aware of the "*essence of the arrangement*". For example, it must be completely clear to a data subject which data controller serves as a point of contact for the exercise of data subject rights (notwithstanding the fact that he or she can exercise his or her rights in respect of and against each joint controller). The obligation to make the essence of the arrangement available to data subjects is important in case of joint controllership in order for the data subject to know which of the controllers is responsible for what.
180. What should be covered by the notion of "*essence of the arrangement*" is not specified by the GDPR. The EDPB recommends that the essence cover at least all the elements of the information referred to in Articles 13 and 14 that should already be accessible to the data subject, and for each of these elements, the arrangement should specify which joint controller is responsible for ensuring compliance with these elements. The essence of the arrangement must also indicate the contact point, if designated.
181. The way such information shall be made available to the data subject is not specified. Contrary to other provisions of the GDPR (such as Article 30(4) for the record of processing or Article 40(11) for the register of approved codes of conduct), Article 26 does not indicate that the availability should be "*upon request*" nor "*publicly available by way of appropriate means*". Therefore, it is up to the joint controllers to decide the most effective way to make the essence of the arrangement available to the data subjects (e.g. together with the information in Article 13 or 14, in the privacy policy or upon request to the data protection officer, if any, or to the contact point that may have been designated). Joint controllers should respectively ensure that the information is provided in a consistent manner.

#### **The arrangement may designate a contact point for data subjects**

182. Article 26(1) provides the possibility for joint controllers to designate in the arrangement a contact point for data subjects. Such designation is not mandatory.
183. Being informed of a single way to contact possible multiple joint controllers enables data subjects to know who they can contact with regard to all issues related to the processing of their personal data. In addition, it allows multiple joint controllers to coordinate in a more efficient manner their relations and communications *vis-à-vis* data subjects.
184. For these reasons, in order to facilitate the exercise of data subjects' rights under the GDPR, the EDPB recommends joint controllers to designate such contact point.
185. The contact point can be the DPO, if any, the representative in the Union (for joint controllers not established in the Union) or any other contact point where information can be obtained.

Irrespective of the terms of the arrangement, data subjects may exercise their rights in respect of and against each of the joint controllers.

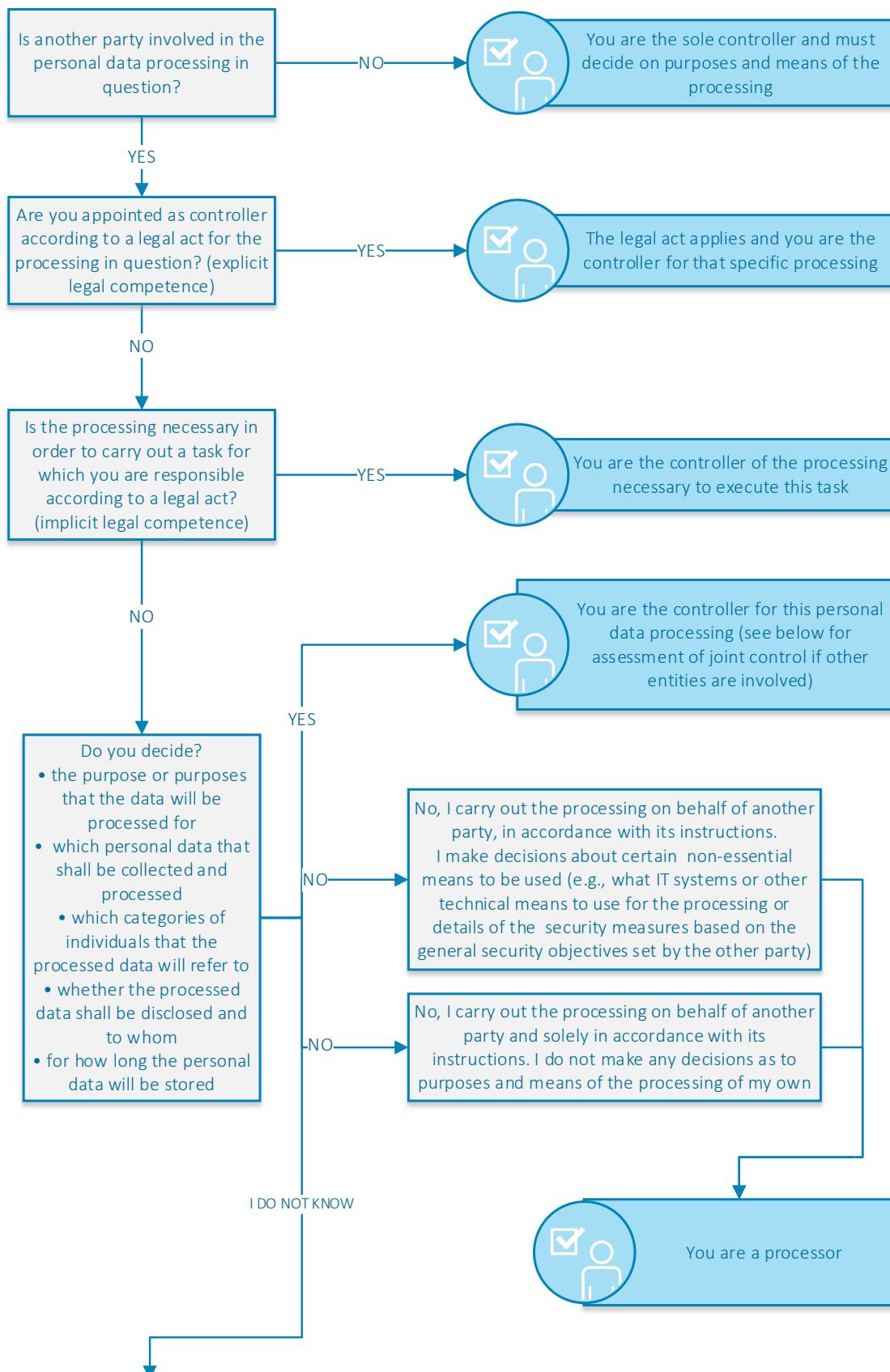
186. Under Article 26(3), a data subject is not bound by the terms of the arrangement and may exercise his or her rights under the GDPR in respect of and against each of the joint data controllers.
187. For example, in case of joint controllers established in different Member States, or if only one of the joint controllers is established in the Union, the data subject may contact, at his or her choice, either the controller established in the Member State of his or her habitual residence or place of work, or the controller established elsewhere in the EU or in the EEA.
188. Even if the arrangement and the available essence of it indicate a contact point to receive and handle all data subjects' requests, the data subjects themselves may still choose otherwise.
189. Therefore, it is important that joint controllers organise in advance in their arrangement how they will manage answers to requests they could receive from data subjects. In this respect, it is recommended that joint controllers communicate to the other controllers in charge or to the designated contact point, the requests received in order to be effectively handled. Requiring data subjects to contact the designated contact point or the controller in charge would impose an excessive burden on the data subject that would be contrary to the objective of facilitating the exercise of their rights under the GDPR.

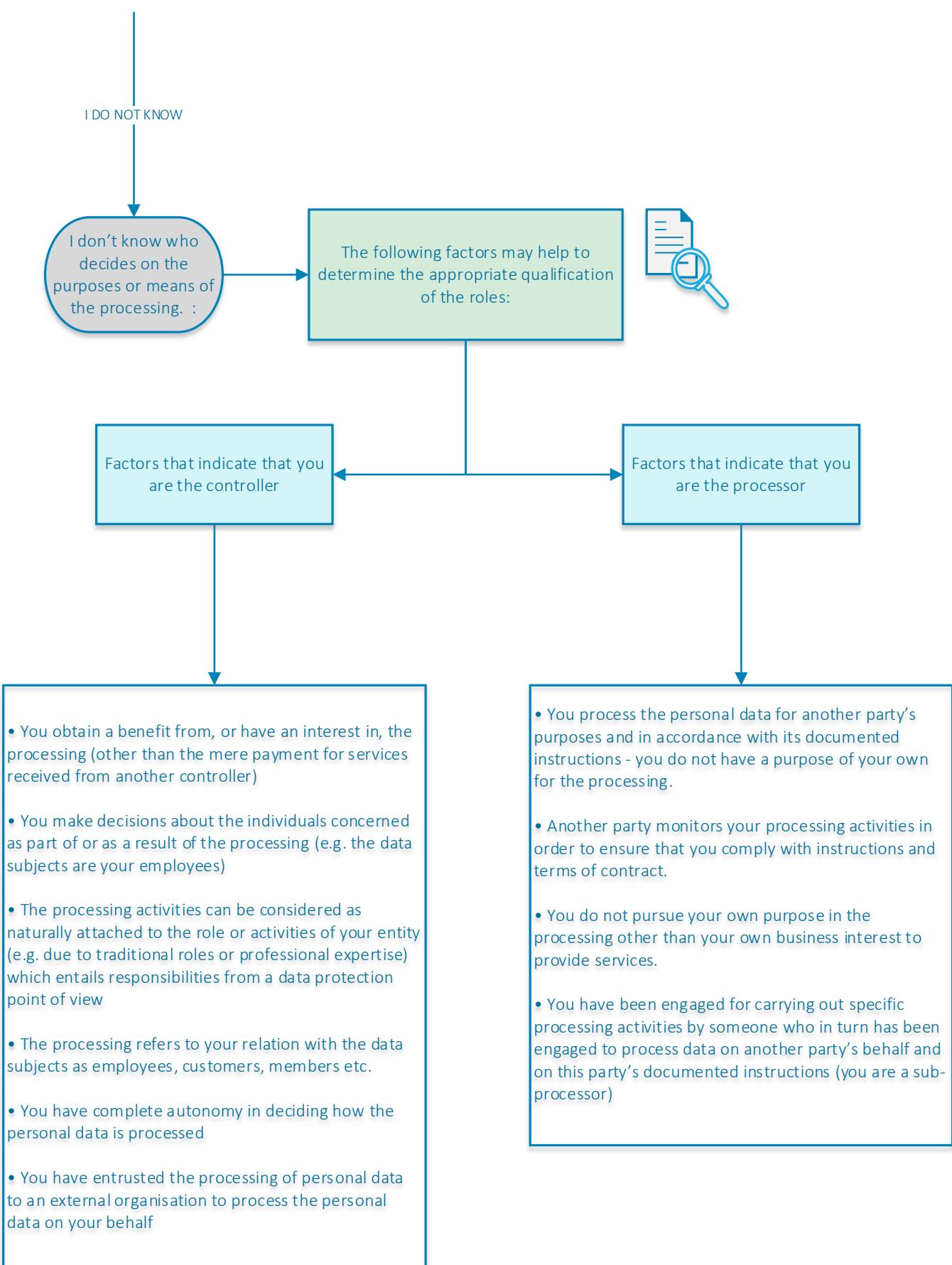
### 2.3 Obligations towards data protection authorities

190. Joint controllers should organise in the arrangement the way they will communicate with the competent supervisory data protection authorities. Such communication could cover possible consultation under Article 36 of the GDPR, notification of a personal data breach, designation of a data protection officer.
191. It should be recalled that data protection authorities are not bound by the terms of the arrangement whether on the issue of the qualification of the parties as joint controllers or the designated contact point. Therefore, the authorities can contact any of the joint controllers to exercise their powers under Article 58 with respect to the joint processing.

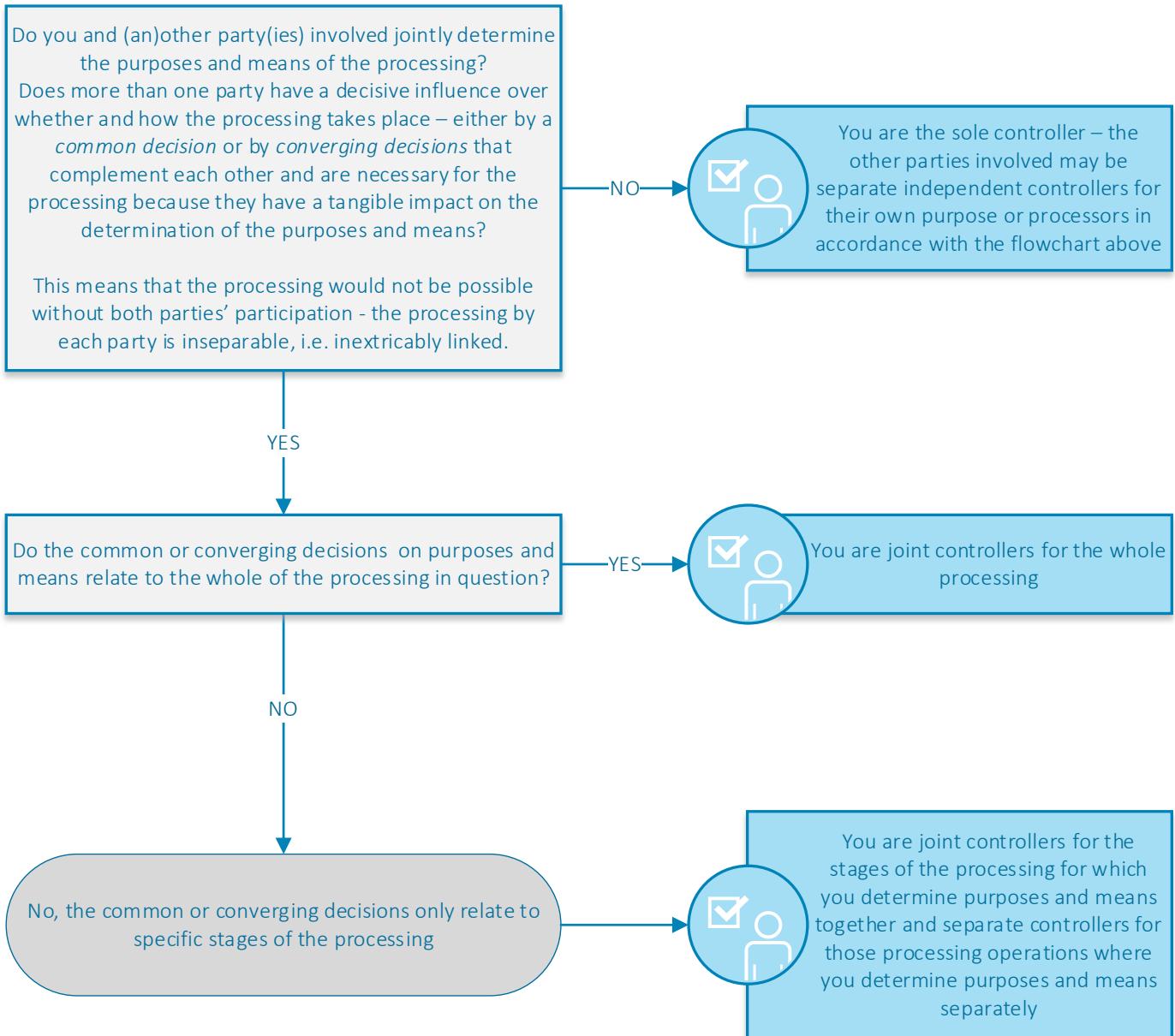
## Annex I – Flowchart for applying the concepts of controller, processor and joint controllers in practice

**Note:** in order to properly assess the role of each entity involved, one must first identify the specific personal data processing at stake and its exact purpose. If multiple entities are involved, it is necessary to assess whether the purposes and means are determined jointly, leading to joint controllership.





**Joint controllership - If you are the controller and other parties are involved in the personal data processing:**



# Guidelines



**Guidelines 09/2020 on relevant and reasoned objection  
under Regulation 2016/679**

**Version 2.0**

**Adopted on 09 March 2021**

## Version Table

Version 1.0	8 October 2020	Adoption of the Guidelines for public consultation
Version 2.0	9 March 2021	Adoption of the Guidelines after public consultation

## Table of contents

1	GENERAL.....	4
2	CONDITIONS FOR A “RELEVANT AND REASONED” OBJECTION.....	6
2.1	“Relevant” .....	6
2.2	“Reasoned” .....	6
3	SUBSTANCE OF THE OBJECTION.....	7
3.1	Existence of an infringement of the GDPR and/or compliance of the envisaged action with the GDPR .....	8
3.1.1	Existence of an infringement of the GDPR .....	8
3.1.2	Compliance with the GDPR of the action envisaged in the draft decision in relation to the controller or processor .....	9
3.2	Significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union	10
3.2.1	Meaning of “significance of the risks”.....	10
3.2.2	Risks to fundamental rights and freedoms of data subjects.....	11
3.2.3	Risks to the free flow of personal data within the Union .....	12

# The European Data Protection Board

Having regard to Article 70(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”),

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,<sup>1</sup>

Having regard to Article 12 and Article 22 of its Rules of Procedure,

## HAS ADOPTED THE FOLLOWING GUIDELINES

### 1 GENERAL

1. Within the cooperation mechanism set out by the GDPR, the supervisory authorities (“SAs”) have a duty to “exchange all relevant information with each other” and cooperate “in an endeavour to reach consensus”.<sup>2</sup> This duty of cooperation applies to every stage of the procedure, starting with the inception of the case and extending to the whole decision-making process. The achievement of an agreement on the outcome of the case is therefore the ultimate goal of the whole procedure established by Article 60 GDPR. In the situations in which no consensus is reached among the SAs, Article 65 GDPR entrusts the EDPB with the power to adopt binding decisions. However, the exchange of information and the consultation among the Lead Supervisory Authority (“LSA”) and the Concerned Supervisory Authorities (“CSAs”) often enables an agreement to be reached at the early stages of the case.
2. According to Article 60(3) and (4) GDPR, the LSA is required to submit a draft decision to the CSAs, which then may raise a relevant and reasoned objection within a specific timeframe (four weeks).<sup>3</sup> Upon receipt of a relevant and reasoned objection, the LSA has two options open to it. If it does not follow the relevant and reasoned objection or is of the opinion that the objection is not reasoned or relevant, it shall submit the matter to the Board within the consistency mechanism. If the LSA, on the contrary, follows the objection and issues the revised draft decision, the CSAs may express a relevant and reasoned objection on the revised draft decision within a period of two weeks.
3. When the LSA does not follow an objection or rejects it as not relevant or reasoned and therefore submits the matter to the Board according to Article 65(1)(a) GDPR, it then becomes incumbent upon the Board to adopt a binding decision on whether the objection is “relevant and reasoned” and if so, on all the matters which are the subject of the objection.
4. Therefore, one of the key elements signifying the absence of consensus between the LSA and the CSAs, is the concept of “relevant and reasoned objection”. This document seeks to provide guidance with

<sup>1</sup> References to “Member States” made throughout this document should be understood as references to “EEA Member States”.

<sup>2</sup> Regulation 2016/679, hereinafter “GDPR”, Article 60(1).

<sup>3</sup> It is possible for the CSAs to withdraw objections previously raised.

respect to this concept and aims at establishing a common understanding of the notion of the terms “relevant and reasoned”, including what should be considered when assessing whether an objection “clearly demonstrates the significance of the risks posed by the draft decision” (Article 4(24) GDPR).

5. Article 4(24) GDPR defines “relevant and reasoned objection” as an *objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union*”.
6. This concept serves as a **threshold** in situations where CSAs aim to object to a (revised) draft decision to be adopted by the LSA under Article 60 GDPR. As the unfamiliarity surrounding “what constitutes relevant and reasoned objection” has the potential to create misunderstandings and inconsistent applications by the supervisory authorities, the EU legislator suggested that the EDPB should issue guidelines on this concept (end of Recital 124 GDPR).
7. In order to meet the threshold set by Article 4(24) GDPR, a submission by a CSA should in principle explicitly mention each element of the definition in relation to each specific objection. Therefore, **the objection aims, first of all, at pointing out how and why, according to the CSA, the draft decision does not appropriately address the situation of infringement of the GDPR, and/or does not envision appropriate action towards the controller or processor in the light of the demonstration of the risks that such draft decision, if left unchanged, would entail for the rights and freedoms of data subjects and for the free flow of personal data in the Union, where applicable**. An objection submitted by a CSA should indicate each part of the draft decision that is considered deficient, erroneous or lacking some necessary elements, either by referring to specific articles/paragraphs or by other clear indications, and showing why such issues are to be deemed “relevant” as further explained below. The proposals for amendments put forward by the objection should aim to remedy these potential errors.
8. Indeed, the **degree of detail of the objection and the depth of the analysis included therein may be affected by the degree of detail in the content of the draft decision and by the degree of involvement of the CSA** in the process leading to the draft decision issued by the LSA. Therefore, the standard of “relevant and reasoned objection” is grounded on the assumption that the LSA’s obligation to exchange all relevant information<sup>4</sup> is complied with, allowing the CSA(s) to have an in-depth understanding of the case and therefore to submit a solid and well-reasoned objection. To this end, the need for each legally binding measure of SAs to “give the reasons for the measure” (see Recital 129 GDPR) should also be kept in mind. The degree of involvement of the CSA by the LSA in the process leading to the draft decision, if it leads to an insufficient knowledge of all the aspects of the case, can therefore be considered as an element to determine the degree of detail of the relevant and reasoned objection in a more flexible way.
9. The EDPB would first like to emphasise that the focus of all SAs involved (LSA and CSAs) should be on eliminating any deficiencies in the consensus-finding process in such a way that a consensual draft decision is the result. Whilst acknowledging that raising an objection is not the most preferable tool to remedy an insufficient degree of cooperation in the preceding stages of the one-stop-shop proceeding, the EDPB nevertheless acknowledges that it is an option open to CSAs. This would be a last resort to also remedy (alleged) deficiencies in terms of CSAs’ involvement by the LSA in the process that should have led to a consensus-based draft decision, including as regards the legal reasoning and the scope of the investigations carried out by the LSA in respect of the case at hand.

---

<sup>4</sup> As per Article 60(1) GDPR.

10. The GDPR requires the CSA to justify its position on the LSA's draft decision by submitting an objection that is "relevant" and "reasoned". It is crucial to bear in mind that the two requirements, "reasoned" and "relevant", are to be deemed **cumulative**, i.e. both of them have to be met.<sup>5</sup> Consequently, Article 60(4) requires the LSA to submit the matter to the EDPB consistency mechanism when it is of the opinion that the objection does not meet at least one of the two elements.<sup>6</sup>
11. The EDPB strongly advises the SAs to raise their objections and exchange information through the information and communication system set up for the exchange of information among SAs.<sup>7</sup> They should be clearly marked as such by using the specific dedicated functions and tools.

## 2 CONDITIONS FOR A "RELEVANT AND REASONED" OBJECTION

### 2.1 "Relevant"

12. In order for the objection to be considered as "relevant", there must be a **direct connection between the objection and the substance of the draft decision at issue**.<sup>8</sup> More specifically, the objection needs to concern either whether there is an infringement of the GDPR or whether the envisaged action in relation to the controller or processor complies with the GDPR.
13. Consequently, the objection raised fulfils the criterion of being "relevant" when, if followed, it would entail a change leading **to a different conclusion** as to whether there is an infringement of the GDPR or as to whether the envisaged action in relation to the controller or processor, as proposed by the LSA, complies with the GDPR. There must always be a link between the content of the objection and such potential different conclusion as further explained below. While it is possible for the objection to signal a disagreement on both elements, the existence of only one of them would be sufficient to meet the conditions for a relevant objection.
14. An objection should only be considered relevant if it relates to specific legal and factual content of the LSA's draft decision. Raising abstract or broad concerns or remarks cannot be considered relevant in this context. Likewise, minor disagreements on the wording or regarding the legal reasoning that do not relate to the possible existence of the infringement nor to the compliance of envisaged action in relation to the controller or processor with the GDPR should not be regarded as relevant.
15. The reasoning underlying the conclusions reached by the LSA in the draft decision can be subject to an objection, but only insofar as such reasoning is linked with the conclusion as to whether there is an infringement, whether the infringement of the GDPR has been correctly identified, or is linked with the compliance of the envisaged action with the GDPR, and to the extent that the whole Article 4(24) threshold as described in this document is met.

### 2.2 "Reasoned"

16. In order for the objection to be "reasoned",<sup>9</sup> it needs to include clarifications and arguments as to **why an amendment of the decision is proposed** (i.e. the legal / factual mistakes of the LSA's draft decision).

---

<sup>5</sup> See the wording of Article 60(4) GDPR.

<sup>6</sup> Pursuant to Article 60(4) GDPR the lead supervisory authority shall also submit the matter to the consistency mechanism referred to in Article 63 if it does not follow the relevant and reasoned objection.

<sup>7</sup> See the EDPB Rules of Procedure.

<sup>8</sup> The Oxford English Dictionary defines "relevant" as "*bearing on or connected with the matter in hand; closely relating to the subject or point at issue; pertinent to a specified thing*" ("relevant, adj." OED Online, Oxford University Press, June 2020, [www.oed.com/view/Entry/161893](http://www.oed.com/view/Entry/161893). Accessed 24 July 2020).

<sup>9</sup> The Oxford English Dictionary defines "reasoned" as "*characterised by or based on reasoning; carefully studied*" ("reasoned, adj.2." OED Online, Oxford University Press, June 2020, [www.oed.com/view/Entry/159078](http://www.oed.com/view/Entry/159078). Accessed 24 July 2020).

It also needs to demonstrate **how the change would lead to a different conclusion** as to whether there is an infringement of the GDPR or whether the envisaged action in relation to the controller or processor complies with the GDPR.

17. The CSA should provide sound and substantiated reasoning for its objection, in particular, by elaborating on **legal arguments** (relying on EU law and/or relevant national law, including e.g. legal provisions, case law, guidelines) **or factual elements**, where applicable. The CSA should present the fact(s) allegedly leading to a different conclusion regarding the infringement of the GDPR by the controller/processor, or the aspect of the draft decision that, in their view, is deficient/erroneous.
18. Moreover, an objection is “reasoned” insofar as it is able to **“clearly demonstrate” the significance of the risks posed by the draft decision** as described in section 3.2 below. To this end, the objection must put forward arguments or justifications concerning the consequences of issuing the decision without the changes proposed in the objection, and how such consequences would pose significant risks for data subjects’ fundamental rights and freedoms, and, where applicable, for the free flow of personal data within the Union.
19. In order for an objection to be adequately reasoned, it should be **coherent, clear, precise and detailed in explaining the reasons for objection**. It should set forth, clearly and precisely, the **essential elements** on which the CSA based its assessment, and the **link between the envisaged consequences of the draft decision** (if it was to be issued as it is) **and the significance of the anticipated risks for data subjects’ fundamental rights and freedoms and, where applicable, for the free flow of personal data within the Union**. Moreover, the CSA should **clearly indicate which parts of the draft decision they disagree with**. In cases where the objection is based on the opinion that the LSA failed to fully investigate an important fact of the case, or an additional violation of the GDPR, it would be sufficient for the CSA to present such arguments in a conclusive and substantiated manner.
20. The CSA(s) must provide all the information (facts, documents, legal arguments) on which they are relying so as to effectively present their argument. This is fundamental in order to delimit the scope of the (potential) dispute. This means that, **in principle, the CSA should aim to provide a relevant and reasoned objection in one single submission** supported by all the factual and legal arguments as described above. However, **within the deadline set forth by Article 60(4) GDPR, the CSA can provide additional information related to and supporting the objection raised, bearing in mind the need to comply with the “relevant and reasoned” requirements**.

**Example 1:** The CSA submits a formal objection, but a few days later provides the LSA with additional information through the information and communication system regarding the facts of the case. Such information may only be taken into consideration by the LSA insofar as it is provided within the deadline set forth by Article 60(4) GDPR.

21. If possible, as a good practice, the objection should include a **new wording proposal** for the LSA to consider, which in the opinion of the CSA allows remedying the alleged shortcomings in the draft decision. This may serve to clarify the objection better in the relevant context.

### 3 SUBSTANCE OF THE OBJECTION

22. The subject matter of the objection may refer to whether there is an infringement of the GDPR and/or to whether the envisaged action in relation of the controller or the processor complies with the GDPR. The type of content will depend on the LSA’s draft decision at stake and on the circumstances of the case.

23. Additionally, the CSA's objection will have to clearly demonstrate the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union. The existence of an infringement and/or the non-compliance of the envisaged action with the GDPR should be assessed in light of the significance of the risks that the draft decision, if left unchanged, poses to the rights and freedoms of data subjects and, if relevant, the free flow of personal data.

### 3.1 Existence of an infringement of the GDPR and/or compliance of the envisaged action with the GDPR

#### 3.1.1 Existence of an infringement of the GDPR

24. In the first case, the substance of the objection will amount to a disagreement between the CSA and the LSA as to whether, in the facts at issue, the activities and processing operations carried out by the controller or processor led to infringement(s) of the GDPR or not, and to which infringement(s) specifically.
25. In this context, the term "infringement" should be interpreted as "an infringement of a given provision of the GDPR". Therefore, the CSA's objections to the draft decision must be justified and motivated through reference to evidence and facts as exchanged between the LSA and the CSAs (the 'relevant information' referred to in Article 60 GDPR). These requirements should apply to each specific infringement and to each specific provision in question.

**Example 2:** The draft decision states that the controller infringed Articles 6, 7, and 14 GDPR. The CSA disagrees on whether there is an infringement of Article 7 and 14 and considers that there is an additional infringement of Article 13 GDPR.

**Example 3:** The CSA argues that LSA did not take into consideration the fact that the household exemption is not applicable to some of the processing operations conducted by a controller and involving the use of CCTV, hence that there is no infringement of the GDPR. In order to justify its objection, the CSA refers to Article 2(2)(c) GDPR, EDPB Guidelines 3/2019 on processing of personal data through video devices, and CJEU case C-212/13 Ryneš.

26. An objection as to whether there is an infringement of the GDPR may also include a disagreement as to the conclusions to be drawn from the findings of the investigation. For instance, the objection may state that the findings amount to the infringement of a provision of the GDPR other than (and/or in addition to) those already analysed by the LSA's draft decision. However, this is less likely to happen when the obligation for the LSA to cooperate with the CSAs and exchange all relevant information in accordance with Article 60(1) GDPR has been duly complied with in the time preceding the issuance of the draft decision.
27. In some circumstances, an objection could go as far as identifying gaps in the draft decision justifying the need for further investigation by the LSA. For instance, if the investigation carried out by the LSA unjustifiably fails to cover some of the issues raised by the complainant or resulting from an infringement reported by a CSA, a relevant and reasoned objection may be raised based on the failure of the LSA to properly handle the complaint and to safeguard the rights of the data subject. In this regard, a distinction must be made between, on one hand, own-volition inquiries and, on the other hand, investigations triggered by complaints or by reports on potential infringements shared by the CSAs. In procedures based on a complaint or on an infringement reported by a CSA, the scope of the procedure (i.e. those aspects of data processing which are potentially the subject of a violation) should be defined by the content of the complaint or of the report shared by the CSA: in other words, it should be defined by the aspects addressed by the complaint or report. In own-volition inquiries, the LSA and

CSAs should seek consensus regarding the scope of the procedure (i.e. the aspects of data processing under scrutiny) prior to initiating the procedure formally. The same applies in cases where a SA dealing with a complaint or report by another SA takes the view that an own-volition inquiry is also necessary to deal with systematic compliance issues going beyond the specific complaint or report.

28. As mentioned above, raising an objection should only be considered as a last resort to remedy an allegedly insufficient involvement of the CSA(s) in the preceding stages of the process. The system designed by the legislator suggests that consensus on the scope of the investigation should be reached at an earlier stage by the competent SAs.
29. The insufficient factual information or description of the case at stake, or the absence or insufficiency of assessment or reasoning (with the consequence that the conclusion of the LSA in the draft decision is not adequately supported by the assessment carried out and the evidence presented, as required in Article 58 GDPR), can also be a matter of objection linked to the existence of an infringement. This is upon the conditions that the whole threshold set forth by Article 4(24) GDPR is met and it is possible that there can be a link between such allegedly insufficient analysis and the finding of an infringement / the envisaged action.
30. It is possible for a relevant and reasoned objection to raise issues concerning procedural aspects to the extent that they amount to situations in which the LSA allegedly disregarded procedural requirements imposed by the GDPR and this affects the conclusion reached in the draft decision.

**Example 4:** The SA of Member State YY is competent to act as LSA for the cross-border processing carried out by the controller CC whose main establishment is in YY. The competent SA of Member State XX informs the LSA (YY) of a complaint lodged with the XX SA substantially affecting data subjects only in XX, pursuant to Article 56(2) and (3) GDPR. The LSA decides to handle the case.

The XX SA decides to submit to the LSA a draft for a decision pursuant to Article 56(4) GDPR. The LSA prepares a draft decision pursuant to Article 60(3) GDPR and submits it to the CSA. The XX SA is of the opinion that the LSA failed to comply with its obligation to take utmost account of the draft submitted by XX SA when preparing its draft decision, pursuant to Article 56(4) GDPR as it does not provide reasoning why it is deviating from the draft for a decision provided by the XX SA.

Subsequently, the XX SA's raises a relevant and reasoned objection in which it puts forward arguments specifying the different conclusion that the draft decision would have reached if the LSA had followed its draft for a decision, in terms of establishing an infringement or determining the actions envisaged vis-à-vis the controller, and with a view to avoiding the demonstrated risks posed to data subject's fundamental rights and freedoms, and, where applicable to the free flow of personal data within the Union.

31. An objection pursuant to Article 60(4) and Article 65(1)(a) GDPR is without prejudice to the provision of Article 65(1)(b) GDPR. Therefore, a disagreement on the competence of the SA acting as LSA to issue a decision in a specific case should not be raised through an objection pursuant to Article 60(4) GDPR, and falls outside the scope of Article 4(24) GDPR. Unlike the objection pursuant to Article 60(4) GDPR, the EDPB considers the procedure pursuant to Article 65(1)(b) GDPR to be applicable at any stage.

### 3.1.2 Compliance with the GDPR of the action envisaged in the draft decision in relation to the controller or processor

32. In this second scenario, the substance of the relevant and reasoned objection amounts to a disagreement regarding the particular corrective measure proposed by the LSA or other action envisaged in the draft decision.

33. More specifically, the relevant and reasoned objection should explain why the action foreseen in the draft decision is not in line with the GDPR. To this end, the CSA must clearly set out factual elements and/or legal arguments underlying the different assessment of the situation, by indicating which action would be appropriate for the LSA to undertake and include in the final decision.

**Example 5:** The controller disclosed sensitive medical data of the complainant to a third party without a legal basis. In the draft decision, the LSA proposed to issue a reprimand, while the CSA provides factual elements showing that the controller is facing broad and systemic issues in its compliance with the GDPR (e.g. it regularly discloses its clients' data to third parties without a legal basis). Therefore it proposes that an order to bring the processing operations into compliance, a temporary ban on the data processing, or a fine should be imposed.

**Example 6:** Due to a mistake of one of its employees, the controller published the name, last name and telephone numbers of all its 100.000 clients on its website. These personal data were publicly accessible for two days. As the controller reacted as soon as possible, the mistake was reported, and all the clients were individually informed, the LSA planned to simply issue a reprimand. One CSA however considers that, due to the large scale of the data breach and its possible impact/risk on the private life of the clients, the imposition of a fine would be required.

34. As enshrined in the last sentence of Article 65 (1)(a) GDPR, the binding decision of the EDPB shall concern all the matters which are the subject of the objection, in particular in case of an infringement. Recital 150 sentence 5 GDPR states that the consistency mechanism may also be used to promote a consistent application of administrative fines. Therefore, it is possible that the objection challenges the elements relied upon to calculate the amount of the fine. If the assessment of the EDPB within this context identifies shortcomings in the reasoning leading to the imposition of the fine at stake, the LSA will be instructed to re-assess the fine and remedy the identified shortcomings. The EDPB's assessment on this matter should be based on common EDPB standards stemming from Article 83(1) and (2) GDPR and the Guidelines on the calculation of administrative fines.

**Example 7:** The CSA considers that the level of the fine envisaged by the LSA in the draft decision is not effective, proportionate or dissuasive, as required by Article 83(1) GDPR, taking into account the facts of the case.

### 3.2 Significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union

#### 3.2.1 Meaning of "significance of the risks"

35. It is important to bear in mind that the goal of the work carried out by SAs is that of protecting the fundamental rights and freedoms of data subjects and facilitating the free flow of personal data within the Union (Articles 4(24) and Article 51 and Recital 123 GDPR).
36. **The obligation to demonstrate the significance of the risks posed by the draft decision (e.g. by the measures provided for therein, or by the absence of corrective measures, etc.) for the rights and freedoms of data subjects and, where applicable, for the free flow of data within the Union lies on the CSA.** The possibility for CSAs to provide such a demonstration will also rely on the degree of detail of the draft decision itself and of the initial provision of information by the LSA, as highlighted above in paragraph 8.

37. "Risk" is mentioned in numerous sections of the GDPR, and previous EDPB guidelines<sup>10</sup> define it as "*a scenario describing an event and its consequences, estimated in terms of severity and likelihood*". Article 4(24) GDPR refers to the need to demonstrate the "significance" of the risks posed by the draft decision, that is, to show the implications the draft decision would have for the protected values. The CSA will need to do so by advancing sufficient arguments to explicitly show that such risks are substantial and plausible, for the fundamental rights and freedoms of data subjects and, where applicable, for the free flow of data in the Union. The demonstration of the significance of the risks cannot be implied from the legal and/or factual arguments provided by the CSA, but it has to be explicitly identified and elaborated in the objection.
38. It should be emphasised that while a relevant and reasoned objection needs to always clearly demonstrate the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects (see Section 3.2.2 below), the demonstration of the risks posed to the free flow of personal data within the European Union is only requested "where applicable" (see below Section 3.2.3).

### 3.2.2 Risks to fundamental rights and freedoms of data subjects

39. The issue at stake concerns the impact the draft decision, as a whole, would have on the data subjects' fundamental rights and freedoms. This may concern the findings the LSA made as to whether the controller or processor infringed the GDPR, and/or the imposition of corrective measures.
40. The approach to be used when assessing the risk posed by the draft decision is not the same as the one applied by a controller in carrying out a data protection impact assessment ("DPIA") to establish the risk of an intended processing operation. Indeed, the subject matter of the assessment is totally different: namely, the effects produced by the conclusions drawn by the LSA as set out in its draft decision regarding whether an infringement has been committed or not. The conclusions of the LSA may entail taking certain measures (the 'envisaged action'). As said, it is by having regard to the draft decision as a whole that such risks are to be demonstrated by the CSA.
41. Recital 129 GDPR clarifies that "*[t]he powers of supervisory authorities should be exercised in accordance with appropriate procedural safeguards set out in Union and Member State law, impartially, fairly and within a reasonable time*" and that "*each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned*".
42. Therefore, the evaluation of the risks posed by the draft decision to the fundamental rights and freedoms of data subjects can rely, *inter alia*, on the appropriateness, necessity, and proportionality of the measures envisaged (or not envisaged) therein as based on the findings related to the existence of an infringement and the possible remedial actions set forth by the controller or processor.
43. Additionally, the risks at stake may refer to the impact of the draft decision on the fundamental rights and freedoms of the data subjects whose personal data are processed by the controller or processor, but also to the impact on the rights and freedoms of data subjects whose personal data might be processed in the future and to the possible reduction of future infringements of the GDPR, where the facts of the case support it.

---

<sup>10</sup> See e.g. WP 248 rev.01 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/67.

**Example 8:** The LSA's draft decision concluded that the principle of data minimisation enshrined in Article 5(1)(c) GDPR was not breached by the controller. The CSA brings factual elements and legal arguments in its objection showing that the processing activity carried out by the controller had actually resulted in a breach of Article 5(1)(c) GDPR, and arguing that a reprimand should be issued against the controller. In order to demonstrate the significance of the risks for the fundamental rights and freedoms of data subjects, the CSA argues that the absence of a reprimand for the violation of a fundamental principle would set a dangerous precedent, by failing to signal the need for a correction of the organisation's data processing activities, and would endanger the data subjects whose personal data are and will be processed by the controller.

### 3.2.3 Risks to the free flow of personal data within the Union

44. Where the objection also refers to these particular risks, the CSA will need to clarify why it is deemed to be "applicable". Additionally, an objection demonstrating risks posed to the free flow of personal data, but not to the rights and freedoms of data subjects, will not be considered as meeting the threshold set by Article 4(24) GDPR.
45. The need to avoid restricting or prohibiting the free movement of personal data for reasons connected with the protection of natural persons with regard to the processing of personal data is explicitly recalled by the GDPR<sup>11</sup>, which aims to introduce harmonised data protection rules across the EU and enable the free flow of personal data within the Union, while ensuring a high level of protection of natural persons' fundamental rights and freedoms, in particular their right to protection of their personal data.
46. The risks to the free flow of personal data within the Union may be created by any measures, including decisions of national SAs, which introduce unjustified limitations regarding data storage (e.g. provisions which oblige a controller to store certain information in a particular Member State) and/or the free flow of personal data between Member States (e.g. through suspension of data flows or imposition of temporary or definitive limitation including a ban on processing).
47. Likewise, the free flow of personal data within the Union may be at risk when expectations are set (or requirements imposed) on how controllers fulfil their obligations under the GDPR, namely in such a way that the actions expected from controllers become tied to a specific region in the EU (e.g. through specific qualifications requirements).
48. Additionally, the free flow of personal data within the Union may also be hampered if unjustifiably different decisions are issued by SAs in situations that are identical or similar (e.g. in terms of sector or type of processing), as a lack of uniformity would endanger the EU level playing field and create contradictory situations within the EU, and a risk of forum shopping. Account should be taken in this respect of national specificities as permitted by the GDPR with regard to certain sectors such as health care, journalism or archives.

---

<sup>11</sup> GDPR, Article 1(3).

# Guidelines



**Guidelines 02/2021 on virtual voice assistants**

**Version 2.0**

**Adopted on 7 July 2021**

## Version history

Version 2.0	7 July 2021	Adoption of the Guidelines after public consultation
Version 1.0	9 March 2021	Adoption of the Guidelines for publication consultation

## EXECUTIVE SUMMARY

A virtual voice assistant (VVA) is a service that understands voice commands and executes them or mediates with other IT systems if needed. VVAs are currently available on most smartphones and tablets, traditional computers, and, in the latest years, even standalone devices like smart speakers.

VVAs act as interface between users and their computing devices and online services such as search engines or online shops. Due to their role, VVAs have access to a huge amount of personal data including all users' commands (e.g. browsing or search history) and answers (e.g. appointments in the agenda).

The vast majority of VVA services have been designed by few VVA designers. However, VVAs can work jointly with applications programmed by third parties (VVA application developers) to provide more sophisticated commands.

To run properly, a VVA needs a terminal device provided with microphones and speakers. The device stores voice and other data that current VVAs transfer to remote VVA servers.

Data controllers providing VVA services and their processors have therefore to consider both the GDPR<sup>1</sup> and the e-Privacy Directive<sup>2</sup>.

These guidelines identify some of the most relevant compliance challenges and provide recommendations to relevant stakeholders on how to address them.

Data controllers providing VVA services through screenless terminal devices must still inform users according to the GDPR when setting up the VVA or installing, or using a VVA app for the first time. Consequently, we recommend to VVA providers/designers and developers to develop voice-based interfaces to facilitate the mandatory information.

Currently, all VVAs require at least one user to register in the service. Following the obligation of data protection by design and by default, VVA providers/designers and developers should consider the necessity of having a registered user for each of their functionalities.

The user account employed by many VVA designers bundle the VVA service with other services such as email or video streaming. The EDPB considers that data controllers should refrain from such practices as they involve the use of lengthy and complex privacy policies that would not comply with the GDPR's transparency principle.

The guidelines consider four of the most common purposes for which VVAs process personal data: executing requests, improving the VVA machine learning model, biometric identification and profiling for personalized content or advertising.

Insofar the VVA data is processed in order to execute the user's requests, i.e. as strictly necessary in order to provide a service requested by the user, data controllers are exempted from the requirement of prior consent under Article 5(3) e-Privacy Directive. Conversely, such consent as required by Article

---

<sup>1</sup> 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").

<sup>2</sup> 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 (hereinafter "e-Privacy Directive").

5(3) e-Privacy Directive would be necessary for the storing or gaining of access to information for any purpose other than executing users' request.

Some VVA services retain personal data until their users require their deletion. This is not in line with the storage limitation principle. VVAs should store data for no longer than is necessary for the purposes for which the personal data are processed.

If a data controller becomes aware (e.g. due to quality review processes) of the accidental collection of personal data, they should verify that there is a valid legal basis for each purpose of processing of such data. Otherwise, the accidentally collected data should be deleted.

VVAs may process data of multiple data subjects. VVA providers/designers should therefore implement access control mechanisms to ensure personal data confidentiality, integrity and availability. However, some traditional access control mechanisms such as passwords are not fit for the VVA context since they would have to be spoken aloud. The guidelines provide some considerations on this regard, including a section specific to the processing special categories of data for biometric identification.

VVA providers/designers should consider that when collecting user's voice, the recording might contain other individuals' voice or data such as background noise that is not necessary for the service. Whenever possible, VVA designers should therefore consider technologies filtering the unnecessary data and ensuring that only the user voice is recorded.

When evaluating the need for a Data Protection Impact Assessment (DPIA), the EDPB considers that it is very likely that VVA services fall into the categories and conditions identified as requiring a DPIA.

Data controllers providing VVA services should ensure users can exercise their data subject rights using easy-to-follow voice commands. VVA providers/designers, as well as app developers should at the end of the process inform users that their rights have been duly factored, by voice or by providing a writing notification to the user's mobile, account or any other mean chosen by the user.

## Table of contents

<b>EXECUTIVE SUMMARY .....</b>	2
1 GENERAL.....	7
2 TECHNOLOGY BACKGROUND .....	8
2.1 Basic characteristics of Virtual Voice Assistants.....	8
2.2 Actors in the VVA ecosystem .....	9
2.3 Step-by-step description .....	10
2.4 Wake-up expressions .....	11
2.5 Voice snippets and machine learning.....	11
3 ELEMENTS OF DATA PROTECTION .....	12
3.1 Legal framework.....	12
3.2 Identification of data processing and stakeholders .....	14
3.2.1 Processing of personal data .....	14
3.2.2 Processing by data controllers and processors .....	15
3.3 Transparency .....	17
3.4 Purpose limitation and legal basis.....	21
3.4.1 Execute users' requests.....	21
3.4.2 Improve the VVA by training the ML systems and manually reviewing of the voice and transcripts.....	22
3.4.3 User identification (using voice data).....	23
3.4.4 User profiling for personalized content or advertising .....	23
3.5 Processing of children's data.....	25
3.6 Data retention .....	25
3.7 Security.....	27
3.8 Processing of special categories of data .....	29
3.8.1 General considerations when processing special categories of data .....	30
3.8.2 Specific considerations when processing biometric data .....	30
3.9 Data minimization .....	32
3.10 Accountability.....	32
3.11 Data protection by design and by default.....	33
4 Mechanisms to exercise Data Subject Rights.....	33
4.1 Right to access .....	34
4.2 Right to rectification.....	35
4.3 Right to erasure .....	35
4.4 Right to data portability .....	36

5	Annex: Automatic Speech Recognition, Speech Synthesis and Natural Language Processing .....	37
5.1	Automatic Speech Recognition (ASR).....	38
5.2	Natural Language Processing (NLP).....	38
5.3	Speech Synthesis .....	38

# The European Data Protection Board

Having regard to Article 70 (1j) and (1e) 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<sup>3</sup>,

Having regard to Article 12 and Article 22 of its Rules of Procedure,

## HAS ADOPTED THE FOLLOWING GUIDELINES

### 1 GENERAL

1. Recent technological advances have greatly increased the accuracy and popularity of virtual voice assistants (VVA). Among other devices, VVAs have been integrated in smartphones, connected vehicles, smart speakers and smart TVs. This integration has given the VVAs access to information of an intimate nature that could, if not properly managed, harm the individuals' rights to data protection and privacy. Consequently, VVAs and the devices integrating them have been under the scrutiny of different data protection authorities.
2. There are several advantages to using speech-based interactions such as: the naturalness of the interaction which does not involve specific learning from the users, the speed of execution of the command and the extension of the field of action which can allow faster access to information. However, relying on speech also brings in difficulties in interpreting the message correctly: variability of the audio signal between different speakers, acoustic environment, ambiguity of the language, etc.
3. In practice, the fluidity or simplification of tasks remains the primary motivation for equipping oneself with VVAs. This may involve, for example, placing/answering a call, setting a timer, etc., especially when the users have their hands unavailable. Home automation is the major application put forward by the designers of VVAs. By proposing to simplify the execution of tasks (turning on the light, adjusting the heating, lowering the shutters, etc.) and to centralize them through a single tool that can be easily activated remotely, they fit into the discourse as a domestic facilitator. In addition to personal or domestic use, voice commands can be of interest in professional environments where it is difficult to handle computer tools and use written commands (e.g. manufacturing work).
4. In theory, the main beneficiaries of the voice interface could be people with disabilities or dependency for whom the use of traditional interfaces is problematic. Virtual voice assistance can provide easier access to information and computer resources and thus promote inclusive

---

<sup>3</sup> References to "Member States" made throughout this document should be understood as references to "EEA Member States".

logics as the use of the voice makes it possible to overcome the difficulties associated with the written word, which can be found among certain classes of users.

5. Finally, health is also an area where there are many cases of use for conversational agents, vocal or not. For instance, during the Covid-19 pandemic, various callbots were deployed to offer a pre-diagnosis to calling users. In the long term some anticipate that the entire patient care process could be impacted by human/assistant interactions: not only for well-being and prevention, but also for treatment and support.
6. There are currently more than 3 billion smartphones and all of them have integrated VVAs, most of them switched on by default. Some of the most widespread operating systems in personal computers and laptops also integrate VVAs. The recent rise of smart speakers (147 million were sold in 2019<sup>4</sup>) is bringing VVAs to millions of homes and offices. However, current VVA designs do not offer by default authentication or access control mechanisms.
7. This document seeks to provide guidance as to the application of the GDPR in the context of the VVAs.

## 2 TECHNOLOGY BACKGROUND

### 2.1 Basic characteristics of Virtual Voice Assistants

8. A VVA can be defined as a software application that provides capabilities for oral dialogue with a user in natural language.
9. Natural language has a semantics specific to human language. Depending on the characteristics of the language and the diversity of the lexicon, the same instruction can be formulated in multiple ways, whereas some commands may seem similar but relate to two different objects. Inference mechanisms are then frequently used to resolve these ambiguities, for example, depending on what has been said previously, the time when the instruction was given, the place, the person's interests, etc.
10. A VVA can be broken down into modules allowing to perform different tasks: sound capture and restitution, automatic speech transcription (speech to text), automatic language processing, dialogue strategies, access to ontologies (data sets and structured concepts related to a given domain) and external knowledge sources, language generation, voice synthesis (text to speech), etc. Concretely, the assistant should allow interaction in order to perform actions (e.g. "turn on the radio", "turn off the light") or to access knowledge (e.g. "what will the weather be like tomorrow?", "is the 7:43 a.m. train running?"). It thus plays the role of intermediary and orchestrator who is supposed to facilitate the accomplishment of the user's tasks.
11. In practice, a VVA is not a smart speaker but a smart speaker can be equipped with a voice assistant. It is common to confuse both of them, however, the latter is only a material incarnation of the former. A VVA can be deployed in a smartphone, a smart speaker, a connected watch, a vehicle, a household appliance, etc.

---

<sup>4</sup> For example, see a press release of 1 August 2019 by the Hamburg Data Protection and Information authority: <https://datenschutz-hamburg.de/pressemitteilungen/2019/08/2019-08-01-google-assistant>

12. The organization of the underlying data processing may involve multiple information flow patterns. It is possible to isolate three main entities:

**The physical instance:** the hardware element in which the assistant is embodied (smartphone, speaker, smart TV, etc.) and which carries microphones, speakers and network and computing capacities (more or less developed depending on the case).

**The software instance:** the part implementing the human-machine interaction strictly speaking and which integrates the modules for automatic speech recognition, natural language processing, dialogue and speech synthesis. This can be operated directly within the physical equipment, but in many cases is performed remotely.

**The resources:** external data such as content databases, ontologies or business applications that provide knowledge (e.g. "tell the time on the West Coast of the United States", "read my emails") or enable the requested action to be carried out in a concrete way (e.g. "increase the temperature by 1.5°C").

13. VVAs allow the installation of third party components or apps that expand their core functionalities. Each VVA names the components differently but all involve the exchange of users' personal data between the VVA designer and the app developer.
14. Although most VVAs do not share the voice snippet with the app developers, these actors still process personal data. Moreover, depending on the nature of the functionality provided, the app developer receives intentions and slots which could include sensitive information like health data.

## 2.2 Actors in the VVA ecosystem

15. A VVA may involve a great number of actors and intermediaries throughout the execution chain. In practice, up to five different actors can be identified. Depending on business models and technological choices, some actors may however take on several combinations of roles, for example, designer and integrator or designer and application developer:

- a. **The VVA provider (or designer):** responsible for the development of the VVA, designs and defines its possibilities and default functionalities: activation modalities, choice of architecture, data access, record management, hardware specifications, etc.
- b. **The VVA application developer:** as for mobile applications, creates applications extending the VVA's default functionalities. To do this, it is necessary to respect the development constraints imposed by the designer.
- c. **The integrator:** manufacturer of connected objects, who wishes to equip them with a VVA. It should respect the requirements defined by the designer.
- d. **The owner:** in charge of physical spaces receiving people (accommodation places, professional environments, rental vehicles, etc.) he/she wishes to provide a VVA to his/her audience (possibly with dedicated applications).
- e. **The user:** final link in the VVA value chain, who can use it on various devices (speaker, TV, smartphone, watch, etc.) depending on how and where the VVA has been deployed and set up.

## 2.3 Step-by-step description

16. In order for a VVA to carry out an action or to access information, a succession of tasks is carried out:
  - 1) Deployed within a piece of equipment (smartphone, loudspeaker, vehicle), the VVA is on standby. To be precise, it is constantly listening. However, until a specific wake-up expression has been detected no audio is transmitted out of the device receiving the voice and no other operation than wake-up expression detection is performed. For this purpose a buffer of a few seconds is used (see following section for more details).
  - 2) The user says the wake-up expression and the VVA locally compares the audio with the wake-up expression. If they match, the VVA opens a listening channel and the audio content is immediately transmitted.
  - 3) In many cases, if the processing of the command is done remotely, a second check of the keyword pronunciation is done on the server side to limit unwanted activations.
  - 4) The user states his request that is transmitted on the fly to the VVA provider. The sequence of speech spoken is then automatically transcribed (speech to text).
  - 5) Using natural language processing (NLP) technologies, the command is interpreted. The intentions of the message are extracted and information variables (slots) are identified. A dialogue manager is then used to specify the interaction scenario to be implemented with the user by providing the appropriate response scheme.
  - 6) If the command involves a functionality provided by a third party app (skill, action, shortcut, etc.), the VVA provider sends to the app developer the intentions and information variables (slots) of the message.
  - 7) A response adapted to the user's request is identified – at least supposedly, the answer “I don't have the answer to your question” being an adapted response in the case the VVA was not able to correctly interpret the request. If necessary, remote resources are used: publicly accessible knowledge databases (online encyclopaedia, etc.) or by authentication (bank account, music application, customer account for online purchase, etc.) and the information variables (slots) are filled with the recovered knowledge.
  - 8) An answer phrase is created and/or an action is identified (lowering the blinds, raising the temperature, playing a piece of music, answering a question, etc.). The sentence is synthesized (text to speech) and/or the action to be performed is sent to the equipment executed.
  - 9) The VVA returns to standby.

Please note that while currently most voice related processing is performed in remote servers, some VVA providers are developing systems that could perform part of this processing locally<sup>5</sup>.

---

<sup>5</sup> This has been reported, for example, here: <https://www.amazon.science/blog/alexa-new-speech-recognition-abilities-showcased-at-interspeech>

## 2.4 Wake-up expressions

17. In order to be used, a VVA should be “awake”. This means that the assistant switches to an active listening mode in order to receive orders and commands from its user. While this wake-up can also sometimes be achieved by a physical action (e.g. by pressing a button, pressing the smart speaker, etc.), almost all VVAs on the market are based on the detection of a wake-up expression or word to switch to active listening mode (also known as activation word or wake-up word / hot word).
18. To do this, the assistant relies on the use of the microphone and slight computational capabilities to detect whether the keyword has been spoken. This analysis, which takes place continuously from the moment the VVA is on, is carried out exclusively locally. Only when the keyword has been recognised are the audio recordings processed for interpretation and execution of the command, which in many cases means sending them to remote servers via the Internet. Keyword detection is based on machine learning techniques. The major challenge in using such methods is that the detection is probabilistic. Thus, for each word or expression pronounced, the system provides a confidence score as to whether the keyword has actually been pronounced. If this score turns out to be higher than a predefined threshold value, this is considered to be the case. Such a system is therefore not free of errors: in some cases activation may not be detected even though the keyword has been said (false rejection) and in other cases activation may be detected even though the user has not said the keyword (false acceptance).
19. In practice, an acceptable compromise should be found between these two types of errors to define the threshold value. However, since the consequence of a false detection of the keyword might be the sending of audio recordings, unexpected and unwanted transmissions of data are likely to occur. Very often, VVA providers implementing remote processing use a two-pass mechanism for this detection: a first pass embedded locally at the equipment level and a second one performed on remote servers where the next data processing are taking place. In this case, developers tend to set up a relatively low threshold in order to enhance the user experience and ensure that when the user says the keyword, it is almost always recognized - even if this means "over-detecting" it - and then implement a second detection pass on the server side, which is more restrictive.

## 2.5 Voice snippets and machine learning

20. VVAs rely on machine learning methods to perform a wide range of tasks (keyword detection, automatic speech recognition, natural language processing, speech synthesis, etc.) and thus necessitate large datasets to be collected, selected, labelled, etc.
21. The over- or under-representations of certain statistical characteristics can influence the development of machine learning-based tasks and subsequently reflect it in its calculations, and thus in its way of functioning. Thus, just as much as its quantity, the quality of the data plays a major role in the finesse and accuracy of the learning process.
22. In order to increase the quality of the VVA and improve the machine learning methods deployed, VVA designers might wish to have access to data relating to the use of the device in real conditions – i.e. voice snippets – in order to work on its improvement.
23. Whether it is to qualify the learning database or to correct errors made when the algorithm is deployed, learning and training of artificial intelligence systems necessarily require human intervention. This part of the work, known as digital labor, raises questions about both working

conditions and safety. In this context, news media have also reported data transfers between VVA designers and subcontractors allegedly without the necessary privacy protection guarantees.

### 3 ELEMENTS OF DATA PROTECTION

#### 3.1 Legal framework

24. The relevant EU legal framework for VVAs is in the first instance the GDPR, as processing of personal data belongs to the core function of the VVAs. In addition to the GDPR, the e-Privacy Directive<sup>6</sup> sets a specific standard for all actors who wish to store or access information stored in the terminal equipment of a subscriber or user in the EEA.
25. In accordance with the definition of "*terminal equipment*"<sup>7</sup>, 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.**<sup>8</sup>
26. Any processing operations of personal data following the aforementioned 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 lawful.<sup>9</sup>
27. Since the controller, when seeking consent for storing or gaining of access to information pursuant to Article 5(3) e-Privacy Directive, will have to inform the data subject about all the purposes of the processing (meaning the "subsequent processing") – including any processing following the aforementioned operations – consent under Article 6 GDPR will generally be the most adequate legal basis to cover the subsequent processing of the personal data. Hence, consent will likely constitute the legal basis both for the storing and gaining of access to information already stored and the processing of personal data following the aforementioned processing operations. Indeed, when assessing compliance with Article 6 GDPR, one should take into account that the processing as a whole involves specific activities for which the EU legislature has sought to provide additional protection.<sup>10</sup> Moreover, controllers must take into account the impact on data subjects' rights when identifying the appropriate lawful basis in

---

<sup>6</sup> 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 (hereinafter "e-Privacy Directive").

<sup>7</sup> Article 1 of Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment, defines "*terminal equipment*" as (a) an "*equipment directly or indirectly connected to the interface of a public telecommunications network to send, process or receive information; in either case (direct or indirect), the connection may be made by wire, optical fibre or electromagnetically; a connection is indirect if equipment is placed between the terminal and the interface of the network;*" (b) *satellite earth station equipment*";

<sup>8</sup> See EDPB Guidelines 1/2020 paragraph 12 for similar reasoning regarding connected vehicles (hereinafter "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.

<sup>9</sup> Ibid, paragraph 41.

<sup>10</sup> Opinion 5/2019, paragraph 41.

order to respect the principle of fairness.<sup>11</sup> The bottom line is that Article 6 GDPR cannot be relied upon by controllers in order to lower the additional protection provided by Article 5(3) e-Privacy directive.

28. As shown in section 2.3 (steps 2 and 3), current VVAs require access to the voice data stored by the VVA device.<sup>12</sup> Therefore, Article 5(3) e-Privacy Directive applies. The applicability of Article 5 (3) e-Privacy Directive means that the storing of information as well as the accessing to information already stored in a VVA requires, as a rule, end-user's prior consent<sup>13</sup> but allows for two exceptions: first, carrying out or facilitating the transmission of a communication over an electronic communications network, or, second, as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.
29. The second exception ("strictly necessary in order to provide an information society service explicitly requested by the subscriber or user") would allow a VVA service provider to process users' data to execute users' requests (see par. 72 in section 3.4.1) without the consent foreseen in Article 5(3) e-Privacy Directive. Conversely, such **consent as required by Article 5(3) ePrivacy Directive would be necessary for** the storing or gaining of access to information for **any purpose other than executing users' request** (e.g. user profiling). Data controllers would need to attribute consent to specific users. Consequently, data controllers should only process non-registered users data to execute their requests.
30. VVAs can accidentally capture audio of individuals who did not intend to use a VVA service. First, to a certain extent and depending on the VVAs, the wake-up expression can be changed. Individuals who are not aware of this change could accidentally use the updated wake-up expression. Second, VVAs can detect the wake-up expression by mistake or by error. It is highly unlikely that either of the exceptions foreseen in Article 5(3) e-Privacy Directive are applicable in the event of an accidental activation. Furthermore, consent as defined in the GDPR must be the "*unambiguous indication of the data subject's wishes*". Thus, it is highly unlikely that an accidental activation could be interpreted as a valid consent. If data controllers become aware (e.g. through automated or human review) that the VVA service has accidentally processed personal data, they should verify that there is a valid legal basis for each purpose of processing of such data. Otherwise, the accidentally collected data should be deleted.
31. Moreover, it should be noted that the personal data processed by VVAs may be highly sensitive in nature. It may carry personal data both in its content (meaning of the spoken text) and its meta-information (sex or age of the speaker etc.). The EDPB recalls that voice data is inherently biometric personal data.<sup>14</sup> As a result, when such data is processed for the purpose of uniquely identifying a natural person or is inherently or determined to be special category personal data, the processing must have a valid legal basis in Article 6 and be accompanied by a derogation from Article 9 GDPR (see section 3.7 below).

---

<sup>11</sup> EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 October 2019, paragraph 1.

<sup>12</sup> It is possible that future VVA devices will adopt the edge computing paradigm and be capable of providing some service locally. In such event, it will be necessary to reassess the applicability of the e-Privacy Directive.

<sup>13</sup> See also EDPB Guidelines 1/2020, paragraph 14.

<sup>14</sup> Article 4(14) GDPR defines biometric data as 'personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data'

### 3.2 Identification of data processing and stakeholders

32. Considering the multiple possibilities of assistance that a VVA can provide in so many different environments of a data subject's daily life,<sup>15</sup> it is worth noting that careful consideration should be taken with the processing of personal data, which can also be impacted by different stakeholders.

#### 3.2.1 Processing of personal data

33. From a personal data protection perspective, several constants can be observed irrespective of the VVA type (i.e. type of device, functionalities, services or combination of them) that can be used by a data subject. Such constants relate to the plurality of personal data, data subjects and data processing at stake.

##### **Plurality of personal data types**

34. The definition of personal data under Article 4(1) GDPR includes a wide variety of different data and applies in a technologically neutral context to any information that relates "*to an identified or identifiable natural person*".<sup>16</sup> Any interaction of a data subject with a VVA can fall under the scope of this definition. Once the interaction takes place, diverse range of personal data may be processed throughout the operation of the VVA as described in section 2.4.
35. From the initial request to the related answer, action or follow-up (e.g. setting up a weekly alert), the first personal data input will therefore generate subsequent personal data. This includes primary data (e.g. account data, voice recordings, requests history), observed data (e.g. device data that relates to a data subject, activity logs, online activities), as well as inferred or derived data (e.g. user profiling). VVAs use speech to mediate between users and all the connected services (e.g. a search engine, an online shop or a music streaming service) but unlike other intermediaries, VVAs may have full access to the requests' content and consequently provide the VVA designer with a wide variety of personal data depending on the purposes of the processing.
36. The plurality of personal data processed when using a VVA, also refers to a plurality of personal data categories for which attention should be paid (see below section 3.7). The EDPB recalls that when special categories of data<sup>17</sup> are processed, Article 9 GDPR requires the controller to identify a valid exemption from the prohibition to processing in Article 9(1) and a valid legal basis under Article 6(1), using an appropriate means identified under Article 9(2). Explicit consent may be one of the appropriate derogations where consent is the legal basis relied on under Article 6(1). Article 9 also notes (in detail) that the Member States may introduce further conditions to processing of biometric or other special categories data.

---

<sup>15</sup> For example: at home, in a vehicle, in the street, at work or in any other private, public or professional spaces or a combination of these spaces.

<sup>16</sup> Article 4(1) GDPR also specifies that "*an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".

<sup>17</sup> Article 9(1) GDPR defines special categories of personal as "*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.*"

### ***Plurality of data subjects***

37. When using a VVA, personal data are processed from the first interaction with the VVA. For some data subjects this refers to the purchase of a VVA and/or the configuration of a user account (i.e. registered users). For other data subjects it refers to the first time they knowingly interact with the VVA of another data subject who purchased and/or configured this VVA (i.e. non-registered users). Besides these two categories of data subjects, there is a third one: accidental users who, registered or not, unknowingly make requests to the VVA (e.g. saying the correct wake-up expression without knowing the VVA is active, or saying other words that are mistakenly identified by the VVA as the wake-up expression).
38. The term plurality of data subjects also refers to multiple users for one VVA (e.g. device shared between registered and non-registered users, between colleagues, in a family, at school) and different types of users based on their condition (e.g. an adult, a child, an elder or a disable person). While a VVA can offer easier interaction with a digital tool and many benefits for some categories of data subjects, it is important to take into consideration the specificities of each category of data subjects and the context of use of the VVA.

### ***Plurality of data processing***

39. The technologies used to provide a VVA also have an impact on the amount of the processed data and the types of processing. The more a VVA provides services or features and is connected to other devices or services managed by other parties, the more the amount of personal data being processed and repurposing processing increases. This results in a plurality of processing carried out by automated means as described in section 2. Besides automated means, some processing may also involve human means. This is the case for example, when the implemented technology involves human intervention, such as the review of transcription of voices into texts, or the provision of annotations on personal data that can be used to insert new models in a machine-learning technology. This is also the case when humans analyse personal data (e.g. metadata) in order to improve the service provided by a VVA.

#### **3.2.2 Processing by data controllers and processors**

40. Data subjects should be in a position to understand and identify the roles at stake and should be able to contact or act with each stakeholder as required under the GDPR. The distribution of roles should not be to the detriment of the data subjects, even though scenarios can be complicated or evolving. In order to assess their roles, stakeholders are referred to the EDPB Guidelines 7/2020 on the concepts of controller and processor in the GDPR.<sup>18</sup>
41. As indicated in paragraph 15, the main stakeholders can be identified under the role of a provider or designer, an application developer, an integrator, an owner, or a combination of them. Different scenarios are possible, depending on who is doing what in the stakeholders' business relationship, on the user's request, the personal data, the data processing activities and their purposes. They should clearly decide and inform data subjects on the conditions under which each of them will act and comply with the resulting roles of controllers, joint-controllers or processors as provided for by the GDPR.<sup>19</sup> Each of them may take on one or

---

<sup>18</sup> EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, V2.0, adopted on 7 July 2021 (hereinafter "Guidelines 7/2020").

<sup>19</sup> GDPR, Articles 12-14, Article 26.

several roles, as they may be a unique data controller, a joint-controller, or a data processor for one data processing whereas carrying out another role for another data processing.

42. From a high-level perspective, the designer may act as a data controller when determining the purposes and means of a processing, but may intervene as a data processor when processing personal data on behalf of other parties, such as an application developer. The VVA user would therefore be subject to several data controllers: the application developer and the designer. It is also possible that the designer, the integrator and the developer are grouped into a single body acting as a unique data controller. In any case, the applicable qualifications have to be established on a case-by-case analysis.

**Example 1:**

The designer of the VVA processes user data for many purposes, including improving the VVA voice comprehension skills and respond accurately to requests. Therefore, and although this purpose may lead to the processing of data resulting from the use of applications provided by third parties, there is only one data controller: the designer of the VVA, on whose behalf and for whose purposes the processing is performed.

**Example 2:**

A bank offers to its customers an application that can be directly queried via the VVA in order to manage their accounts.

Two actors are involved in the processing of personal data: the designer of the VVA and the developer of the banking application.

In the scenario presented, the bank is the data controller for the provision of the service since it determines the purposes and essential means of processing related to the application allowing interaction with the assistant. Indeed, it offers a dedicated application that allows the user, a customer of the bank, to manage his/her accounts remotely. In addition, it decides on the means of processing by choosing appropriate processor, which is the designer of the VVA and can play an important role in assisting with its expertise to determine these means (for example, it can operate the development platform that allows third-party applications to be integrated into the VVA and, therefore, sets the framework and conditions to be respected by application developers).

43. On the data subject side, it is worth noting that several stakeholders may process the same personal data, even if the data subject does not really expect other parties than the VVA provider to be involved in the processing chain. So when a data subject acts with the VVA provider in relation to his/her personal data (e.g. exercise of data subject's rights), this does not automatically mean that this action will apply to the same personal data that is processed by another stakeholder. When these stakeholders are independent controllers, it is important that a clear information notice is given to the data subjects, explaining the various stages and actors of the processing. Moreover, in cases of joint controllership, it should be made clear if every controller is competent to comply with all data subject's rights or which controller is competent for which right.<sup>20</sup>

---

<sup>20</sup> Guidelines 7/2020, par. 165.

**Example 3:**

In this scenario, the designer of the VVA wishes to use the data collected and processed for the service provided by the bank in order to improve its voice recognition system. The designer of the VVA, who processes the data for its own purposes, will then have the status of controller for this specific processing.

44. As many stakeholders may be involved in the processing chain, and respectively many staff, risky situations may occur if no appropriate measures and safeguards are in place. Controllers are accountable for them and therefore should focus on protecting personal data, notably by choosing appropriate business partners and data processors, applying privacy by default and by design principles,<sup>21</sup> implementing adequate security and other GDPR tools such as audits and legal agreements (e.g. Articles 26 for joint controllers or 28 GDPR for processors).
45. VVA ecosystem is a complex one, where potentially many actors could exchange and process personal data as data controllers or processors. It is of utmost importance to clarify the role of each actor in respect of each processing and to follow the data minimisation principle also in respect of the data exchange.
46. In addition, controllers should be vigilant on personal data transfers and guarantee the required level of protection throughout the processing chain, in particular when they use services located outside of the EEA.

### 3.3 Transparency

47. Since VVAs process personal data (e.g. users' voice, location or the content of the communication), they must comply with the transparency requirements of the GDPR as regulated in Article 5 (1) (a) as well as Article 12 and Article 13 (enlightened by Recital 58). Data controllers are obliged to inform users of the processing of their personal data in a concise, transparent, intelligible form, and in an easily accessible way.
48. Failure to provide necessary information is a breach of obligations that may affect the legitimacy of the data processing. Complying with the transparency requirement is an imperative, since it serves as a control mechanism over the data processing and allows users to exercise their rights. Informing users properly on how their personal data is being used makes more difficult for data controllers to misuse the VVA for purposes that go far beyond user expectations. For example, patented technologies aim to infer health status and emotional states from a user's voice and adapt the services provided accordingly.
49. Complying with the transparency requirements can be particularly difficult for the VVA service provider or any other entity acting as data controller. Given the specific nature of VVAs, data controllers face several obstacles to comply with the GDPR's transparency requirements:
  - | **Multiple users:** data controllers should inform all users (registered, non-registered and accidental users), not only the user setting up the VVA.

---

<sup>21</sup> See EDPB 4/2019 Guidelines on Article 25 Data Protection by Design and by Default, Version 2.0, adopted on 20 October 2020.

- J **Ecosystem complexity:** as explained in the technology background section, the identities and roles of those processing personal data when using a VVA is far from evident for the users.
  - J **Specificities of the vocal interface:** digital systems are not yet fit for voice-only interactions as the almost systemic use of a companion screen proves. However, adapting to the vocal interface and being able to inform the user clearly and correctly through this means is a necessity.
50. VVAs can be regarded as finite states machines going through a number of states during their ordinary functioning. They can be listening locally for the detection of wake-up expressions, or interacting with a remote server to resolve a command, but they can assume many other states depending on the context (e.g. if there is background environmental sound) or the user talking to them (e.g. they may talk to an identified or unknown user). Unfortunately, these situations take place in a substantial asymmetry of information with the user, who is hardly aware if the device is listening, and even less on the status in which it lies.
51. It is highly recommended that VVA designers and developers take adequate steps to fill those asymmetries, making the functioning of VVAs more interactive. Users should be informed of the status in which the device currently lies. This enhancement in transparency can be achieved both making the dialogue man-machine more interactive (e.g. the device might acknowledge in some way the reception of a vocal command), or broadcasting the status of the machine with specific signals. There are many options that can be explored in this regard, ranging from the use of specific vocal acknowledgements and visible icons or lights, or the use of displays on the device.
52. These issues are especially relevant considering the plurality of users and the presence among them of vulnerable categories of individuals, such as children, elderly people or users with audio-visual disabilities.
53. Two important questions become evident from the issues above: what is the most feasible way to inform users and when is the appropriate time to inform them? These issues should be further examined in two different situations, depending on whether the VVA has only one user (such as a personal smart phone) or potentially multiple users (e.g. smart home device). Using the VVA technology, a subversion of these two basic settings could also occur, e.g. when a user has a personal smart phone and connects this to a car. The VVA of the smart phone, which could reasonably be expected to be used by that user only, is now “extended” to the others in the car.
54. Currently, all VVAs are connected to a user account and/or are set up by an application that requires one. The question of how data controllers could consider informing these users about the privacy policy while setting up the VVA should be addressed as described in the Article 29 Working Party Guidelines on transparency. Apps should make the necessary information available in an online store prior to download<sup>22</sup>. This way the information is given the earliest time possible and at the latest, at the time the personal data is obtained. Some VVA providers include third-party apps in the VVA default setup so these apps can execute those apps by using specific wake up expressions. VVAs using this third-party app deployment strategy should ensure that users get the necessary information also on the third-party processing.

---

<sup>22</sup> Guidelines on transparency under Regulation 2016/679, WP260 rev. 01, endorsed by EDPB (hereinafter “WP29 Guidelines WP260”), paragraph 11.

55. However, many VVA designers require VVA user accounts that bundle the VVA service with multiple other services like email, video streaming or purchases to name a few. The decision by the VVA designer of linking the account to many different services has the effect of requiring very lengthy and complex privacy policies. The length and complexity of such privacy policies greatly hinder fulfilling the transparency principle.

**Example 4:**

A VVA designer requires its users to have an account to access the VVA service. This user account is not specific to the VVA service and can be used for other services offered by the VVA designer such as email, cloud storage and social media. To create the account, users have to read and accept a 30 pages long privacy policy. The policy includes information on the processing of personal data by all the services that could be linked with the account.

The information provided by the VVA designer in this case should not be deemed as concise and its complexity reduces the required transparency. Therefore, the VVA designer would not be complying with the transparency requirements as set out in Articles 12 and 13 GDPR.

56. Although the most common way to provide necessary information is in writing, the GDPR allows “other means” as well. Recital 58 explicitly states that the information can be given in electronic form, e.g. through a website. In addition, when choosing the appropriate method to inform the data subjects, account should be taken to the specific circumstances, such as the manner the data controller and the data subject otherwise interact with each other.<sup>23</sup> An option for devices without a screen could be to provide a link which is easy to understand, either directly or in an e-mail. Already existing solutions could serve as example for the information, e.g. call centres’ practices of notifying the caller about a phone call being recorded and directing them to their privacy policies. The constraints of screen less VVA does not exempt the data controller from providing the necessary information according to the GDPR when setting up the VVA or installing or using a VVA app. VVA providers and developers should develop voice-based interfaces to facilitate the mandatory information.
57. VVAs could be of great interest for users with impaired vision since they provide an alternative interaction means with the IT services that traditionally rely on visual information. According to Article 12 (1) GDPR providing the necessary information orally is possible exclusively if requested so by the data subject, but not as the default method. However, the constraints of screen less VVAs would require automated oral information means that could be augmented by written means. When using audio to inform data subjects, data controllers should provide the necessary information in a way that is concise and clear. Furthermore, data subjects should be able to re-listen<sup>24</sup>.
58. Taking the appropriate measures to comply with GDPR transparency requirements is more complex when there are multiple users of the VVA other than the owner of the device. VVA designers must consider how to properly inform non-registered and accidental users when their personal data is processed. When consent is the legal basis for processing users’ data, users must be properly informed for the consent to be valid<sup>25</sup>.

---

<sup>23</sup> WP29 Guidelines WP260, paragraph 19.

<sup>24</sup> WP29 Guidelines WP260, paragraph 21.

<sup>25</sup> GDPR, Article 4 (11).

59. In order to comply with the GDPR, data controllers should find a way to inform not only registered users, but also non-registered users and accidental VVA users. These users should be informed at the earliest time possible **and at the latest, at the time of** the processing. This condition could be especially difficult to fulfil in practice.
60. Certain corporate specificities should also not be detrimental to the data subjects. As many stakeholders are global companies or are well known for a specific business activity (e.g. telecommunication, e-commerce, information technologies, web activities), the way they provide a VVA service should be clear. Adequate information should make the data subjects understand whether or not their use of the VVA will be linked to other processing activities managed by the VVA service provider (e.g. telecommunication, e-commerce, information technologies or web activities) apart from the strict use of the VVA.

**Example 5:**

To use its assistant, a VVA designer which also provides a social media platform and a search engine, requires the user to link his/her account to the assistant. By linking his/her account to the use of the VVA, the designer can thus enhance the profile of its users through the use of the assistant, the applications (or skills) that are installed, the orders placed, etc. Hence assistant interactions are a new source of information attached to a user. VVA designer should provide users' with clear information as to how their data will be processed for each service and with controls allowing the user to choose if the data will be used or not for profiling.

## Recommendations

61. When users are informed about the VVA processing of personal data using a user account's privacy policy and the account is linked to other independent services (e.g. email or online purchases), the EDPB recommends the privacy policy to have a clearly separated section regarding the VVA processing of personal data.
62. The information provided to the user should match the exact collection and processing that is carried out. While some meta-information is contained in a voice sample (e.g. stress level of the speaker), it is not automatically clear, whether such analysis is performed. It is crucial that controllers are transparent on what specific aspects of the raw data they process.
63. Furthermore it should at all times be apparent which state the VVA is in. Users should be able to determine whether a VVA is currently listening on its closed-loop circuit and especially whether it is streaming information to its back-end. This information should also be accessible for people with disabilities such as colour blindness (daltonism), deafness (anacusia). Specific care should be given to the fact that VVAs suggest a usage scenario where eye-contact to the device is not necessary. So, all user feedback, including state changes should be available in visual and acoustic form at least.
64. Particular consideration should be applied if devices allow adding third party functionality ("apps" for VVAs). While some general information can be given to the user when they are the ones adding such functionality (given that it is the user's choice), during normal use of the device, the boundaries between the various controllers involved can be much less clear, i.e. the user might be not sufficiently informed how and by whom their data is processed (and to which extent) in a specific query.

65. All information about processing based on data collected and derived from the processing of recorded voice should also be available to users according to article 12 GDPR.
66. VVA controllers should make transparent what kind of information a VVA can derive about its surroundings, such as but not limited to other people in the room, music running in the background, any processing of the voice for medical or marketing other reasons, pets, etc.

### 3.4 Purpose limitation and legal basis

67. The processing of voice requests by VVAs has an evident purpose, the execution of the request. However, there often are additional purposes which are not so evident, like the improvement of the VVA natural language understanding capacities by training VVA model with machine learning techniques. Among the most common purposes for processing personal data by VVAs we find:
  - | Execute users' requests
  - | VVA improvement by training of the machine learning model and human review and labelling of voice transcriptions
  - | User identification (using voice data)
  - | User profiling for personalized content or advertising
68. Due to their role as intermediaries and the way they are designed, VVAs process a wide variety of personal and non-personal data. This allows processing personal data for many purposes that go beyond answering the users' requests and that could go totally unnoticed. By analysing data collected via VVAs, it is possible to know or infer user interests, schedules, driving routes or habits. This could enable personal data processing for unforeseen purposes (e.g. sentiment analysis or health condition assessment<sup>26</sup>), which would be far beyond the reasonable user expectations.
69. Data controllers should clearly specify their purpose(s) in relation to the context in which the VVA is used, so that they are clearly understood by the data subjects (e.g. presenting purposes in categories). In line with Article 5(1) GDPR, the personal data should be collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with these purposes.

#### 3.4.1 Execute users' requests

70. The main use for a VVA is to issue voice commands that need to be executed by the VVA or an associated app or service (e.g. a music streaming service, a mapping service or an electronic lock). The user's voice and potentially other data (e.g. the user's position when requesting a route for a certain destination) might therefore be processed.

**Example 6:**

The passenger of a smart car including a VVA requests a route to the closest gas station. The VVA processes the user voice to understand the command and the car's position to find the route and sends it to the smart component to show it in the car's screen.

71. Insofar as the processing of voice commands involves the storage or access to information stored in the terminal devices of the end-user, Article 5(3) of the e-Privacy Directive must be

---

<sup>26</sup> Eoghan Furey, Juanita Blue, "Alexa, Emotion, Privacy and GDPR", Conference paper, Human Computer Interaction Conference, July [2018].

complied with. While Article 5(3) includes the general principle that such storage or access requires the prior consent of the end-user, it also provides for an exemption to the consent requirement where it is “strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service”. Insofar as the voice data is processed in order to execute the user’s requests, it is exempted from the requirement of prior consent.

72. As indicated earlier, any processing operations of personal data subsequent to the storage or access to information in the terminal device of end-users must have a legal basis under Article 6 GDPR to be lawful.
73. There are two consecutive processing operations taking place on the VVA. As mentioned above the first one requires access to the VVA (and therefore the conditions of Article 5(3) e-Privacy Directive must be met). In addition to the conditions of Article 5(3) e-Privacy Directive, this second step also requires a legal basis under Article 6 GDPR.
74. When an individual takes the decision to use a VVA, this action generally implies that the initial user first needs to register an account to activate the VVA. In other words, this situation refers to a contractual relationship<sup>27</sup> between the registered user and the VVA controller. In view of its substance and fundamental objective, the core purpose of this contract is to use the VVA in order to execute the user’s request of assistance.
75. Any personal data processing that is necessary to execute the user’s request can therefore rely on the legal basis of the performance of the contract<sup>28</sup>. Such processing notably includes the capture of the user’s voice request, its transcription to text, its interpretation, the information exchanged with knowledge sources to prepare the reply and then, the transcription to a vocal final reply that ends the user’s request.
76. Performance of a contract can be a legal basis for processing personal data using machine learning (ML) when it is necessary for the provision of the service. Processing personal data using ML for other purposes which are not necessary such as service improvement should not rely on that legal basis.
77. Last but not least, the legal bases of the performance of the contract and consent under the GDPR should not be confused. The consent provided for entering into, i. e. agreeing to the contract is part of the validity of this contract and does not refer to the specific meaning of the consent under the GDPR<sup>29</sup>.
78. When using a VVA does not require to previously configure a user account to the VVA, consent could be a possible legal basis.

### 3.4.2 Improve the VVA by training the ML systems and manually reviewing of the voice and transcripts

79. The accents and variations of human speech are vast. While all VVAs are functional once out of the box, their performance can improve by adjusting them to the specific characteristics of

---

<sup>27</sup> Provided that “*the contract is valid pursuant to applicable national contract laws*”, extract from Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects (“Guidelines 2/2019”), §26.

<sup>28</sup> In accordance with the Guidelines 2/2019, which moreover states that the Opinion 06/2014 remains relevant to Article 6(1)(b) and the GDPR (see in particular pages 11, 16, 17, 18 and 55 in this Opinion 06/2014).

<sup>29</sup> See Guidelines 2/2019, respectively §18, §19, §20, §21 and §27.

users' speech. As mentioned in section 2.6, this adjustment process relies on machine learning methods and consists of two processes: adding to the VVA training dataset new data collected from its users and the human review of the data processed for the execution of a fraction of the requests.

**Example 7:**

A VVA user has to issue three times the same voice command due to the VVA not understanding it. The three voice commands and the associated transcriptions are passed to human reviewers to review and correct the transcriptions. The voice commands and reviewed transcriptions are added to the VVA training dataset to improve its performance.

80. The processing activities described in the example should not be considered as (strictly) "*necessary for the performance of a contract*" within the meaning of Article 6(1)(b) GDPR, and therefore require another legal basis from Article 6 GDPR. The main reason being that VVAs are already functional when they come out of the box and can already perform as (strictly) necessary for the performance of the contract. The EDPB does not consider that Article 6(1)(b) would generally be an appropriate lawful basis for processing for the purposes of improving a service or developing new functions within an existing service. In most cases, a user enters into a contract to avail of an existing service. While the possibility of improvements and modifications to a service may routinely be included in contractual terms, such processing usually cannot be regarded as being objectively necessary for the performance of the contract with the user.

#### 3.4.3 User identification<sup>30</sup> (using voice data)

81. The use of voice data for user identification implies the processing of biometric data as defined in Article 4.14 of the GDPR. Consequently, the data controller will need to identify an exemption under Article 9 of the GDPR in addition to the identification of a legal basis under Article 6 of the GDPR<sup>31</sup>.
82. Of the exemptions listed in Article 9 of the GDPR, only data subjects' explicit consent seems applicable for this specific purpose.
83. However, since this purpose requires to apply the specific legal regime of article 9 of the GDPR further details follow in the section 3.8, related to the processing of special categories of data.

#### 3.4.4 User profiling for personalized content or advertising

84. As mentioned above, VVAs have access to the content of all voice commands even when they are aimed at services provided by third parties. This access would enable the VVA designer to

---

<sup>30</sup> Technically, the notion of identification has to be distinguished from verification (authentication). Identification is a one-to-many (1: N) search and comparison and requires in principle a database in which several individuals are listed. Differently, the processing for verification purposes is a one-to-one (1:1) comparison and is used to verify and to confirm by a biometric comparison whether an individual is the same person as the one from whom the biometric data originates. To the knowledge of the EDPB, VVA on the market rely on the sole use of speaker identification technologies.

<sup>31</sup> GDPR considers that the mere nature of data is not always sufficient to determine if it qualifies as special categories of data since "*the processing of photographs [...] are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person*" (recital 51). The same reasoning applies to voice.

construct very accurate user profiles that could be used to offer personalized services or advertisements.

**Example 8:**

Each time a VVA user makes an Internet search, the VVA adds labels signalling topics of interest to the user profile. The results for each new search are presented to the user ordered taking into account those labels.

**Example 9:**

Each time a VVA user makes a purchase from an e-commerce service, the VVA stores a record of the purchase order. The VVA provider enables third parties to target the VVA user with targeted advertisements on the basis of past purchases.

85. Personalisation of content may (but does not always) constitute an intrinsic and expected element of a VVA. Whether such processing can be regarded as an intrinsic aspect of the VVA service will depend on the precise nature of the service provided, the expectations of the average data subject in light not only of the terms of service but also the way the service is promoted to users, and whether the service can be provided without personalisation.<sup>32</sup>
86. Where personalisation takes place in the context of a contractual relationship and as part of a service explicitly requested by the end-user (and the processing is limited to what is strictly necessary to provide this service), such processing may be based on article 6(1)(b) of the GDPR.
87. If processing is not strictly “*necessary for the performance of a contract*” within the meaning of Article 6(1)(b) GDPR, the VVA provider must, in principle, seek the consent of the data subject. Indeed, because consent will be required under Article 5(3) of the e-Privacy directive for the storing or gaining of access to information (see paragraphs 28-29 above), consent under Article 6(1)(a) GDPR will also, in principle, be the appropriate legal basis for the processing of personal data following those operations as reliance on legitimate interest could, in certain cases, risk undermining the additional level of protection provided by Article 5(3) of the e-Privacy directive.
88. Regarding user profiling for advertisement, it should be noted that this purpose is never considered as a service explicitly requested by the end-user. Thus, in case of processing for this purpose users’ consent should be systematically collected.

## Recommendations

89. Users should be informed of the purpose of processing personal data and that purpose should accord with their expectations of the device they purchase. In case of a VVA, that purpose – from a user’s point of view – clearly is the processing of their voice for the sole purpose of interpreting their query and provide meaningful responses (be that answers to a query or other reactions like remote-controlling a light switch).
90. When the processing of personal data is based on consent, such consent “*should be given in relation to one or more specific purposes and that a data subject has a choice in relation to each of them*”. Moreover, “*a controller that seeks consent for various different purposes should*

---

<sup>32</sup> See also Guidelines 2/2019, paragraph 57.

*provide a separate opt-in for each purpose, to allow users to give specific consent for specific purposes*<sup>33</sup>. For example, users should be able to separately consent or not for the manual review and labelling of voice transcriptions or the use of their voice data for user identification/authentication (see section 3.7).

### 3.5 Processing of children's data

91. Children can also interact with the VVAs or can create their own profiles connected to the ones of the adults. Some VVAs are embedded in devices which are specifically aimed at children.
92. When the legal basis for the processing is the performance of a contract, the conditions for processing children data will depend on national contract laws.
93. When the legal basis for the processing is consent and according to Article 8(1) GDPR, processing of children's data is only lawful "*where the child is at least 16 years old. Where the child is below the age of 16 years, such processing should be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child*". Consequently, to comply with the GDPR, when consent is the legal basis, explicit permission should be sought from parents or guardians to collect, process, and store children's data (voice, transcripts, etc.).
94. Parental controls are available to a certain degree but in their current form they are not user friendly (e.g. it is necessary to sign in a new service) or have limited capacities. Data controllers should invest in developing means for parents or guardians to control children use of VVAs.

### 3.6 Data retention

95. VVAs process and generate a wide variety of personal data like voice, transcriptions of voice, metadata or system logs. These types of data could be processed for a wide range of purposes like provision of a service, NLP improvement, personalization or scientific research. Following the GDPR data storage limitation principle, VVAs should store data for no longer than is necessary for the purposes for which the personal data are processed. Therefore, the data retention periods should be tied to different processing purposes. VVA service providers or third-parties providing services through VVAs should assess the maximum retention period for each data set and purpose.
96. The data minimization principle is closely related to the data storage limitation principle. Not only do data controllers need to limit the data storage period, but also the type and quantity of data.
97. Data controllers should ask themselves, among others the following questions: Is it necessary to store all voice recordings or all transcriptions to achieve the purpose X? Is it necessary to store the voice data once the transcription has been stored? In that case, for what purpose? How long is voice or transcription data necessary for each purpose? The answer to these and other similar questions will define the retention periods that should be part of the information available to the data subjects.
98. Some VVA store by default personal data like voice snippets or transcriptions for an undefined period while providing users means to delete such data. Retaining personal data indefinitely goes against the storage limitation principle. Providing data subjects with means to delete

---

<sup>33</sup> See EDPB [Guidelines 05/2020 on consent under Regulation 2016/679](#), adopted on 4 May 2020, section 3.2.

their personal data does not remove the data controller's responsibility of defining and enforcing a data retention policy.

99. VVA design needs to take into account users' controls to delete their personal data in their devices and in all remote storage systems. These controls may be required to resolve different kind of users' requests, for example, a request of erasure or the withdrawal of previously given consent. The design of some VVAs did not take into account this requirement.<sup>34</sup>
100. As in other contexts, data controllers may need to retain personal data as evidence of a service provided to a user to comply with a legal obligation. The data controller may retain personal data based on that basis. However, the data retained should remain the minimum necessary to comply with such a legal obligation and for the minimum amount of time. Of course, the data retained for the purpose of complying with a legal obligation should not be used for any other purposes without a legal basis under Article 6 GDPR.

**Example 10:**

A user purchases a TV in an e-commerce service using a voice command issued to a VVA. Even if the user requests afterwards the deletion of their data, the VVA provider or developer could still retain some data on the grounds of their legal obligation set by tax regulation to keep purchase evidence. However, the data stored for this purpose should not exceed the minimum necessary to comply with the legal obligation and could not be processed for any other purposes without a legal basis under Article 6 GDPR.

101. As mentioned in section 2, VVAs voice recognition capacity improves by training machine learning systems with users' data. If users do not consent or withdraw their consent to the use of their data for such purpose, their data could not be lawfully used to train any more model and should be deleted by the data controller, assuming that there is no other purpose justifying the continued retention. However, there is evidence that there may be risks of re-identification in some machine learning models.<sup>35</sup>
102. Data controllers and processors should use models which do not restrict their ability to stop processing if an individual revokes their consent, nor should they use models which restrict their ability to facilitate data subject rights. Controllers and processors should apply mitigation measures to reduce the re-identification risk to an acceptable threshold.
103. In the event that the user withdraws his or her consent, the data collected from the user can no longer be used for further training of the model. Nevertheless, the model previously trained using this data does not have to be deleted. The EDPB however highlights that there is evidence that there may be risks of personal data leaking in some machine learning models. In particular, numerous studies showed that reconstruction as well as membership inference attacks can be performed, allowing attackers to retrieve information about individuals.<sup>36</sup> Data controllers and processors should therefore apply mitigation

<sup>34</sup> See Amazon's letter of 28 June 2019 in response to US Senator Christopher Coons: [https://www.coons.senate.gov/imo/media/doc/Amazon%20Senator%20Coons\\_Response%20Letter\\_6.28.19\[3\].pdf](https://www.coons.senate.gov/imo/media/doc/Amazon%20Senator%20Coons_Response%20Letter_6.28.19[3].pdf)

<sup>35</sup> Veale Michael, Binns Reuben and Edwards Lilian 2018 "Algorithms that remember: model inversion attacks and data protection law" Phil. Trans. R. Soc. A.37620180083, doi: 10.1098/rsta.2018.0083

<sup>36</sup> N. Carlini et al, "Extracting Training Data from Large Language Models" Dec 2020.

measures to reduce the re-identification risk to an acceptable threshold to make sure they use models which do not contain personal data.

104. Data subjects should not be nudged to keep their data indefinitely. While deleting stored voice data or transcriptions might have an impact on the service performance, such impact should be explained to users in a clear and measurable way. VVA service providers should avoid making general statements on the degradation of the service after personal data is deleted.
105. Anonymizing voice recordings is specially challenging, as it is possible to identify users through the content of the message itself and the characteristics of voice itself. Nevertheless, some research<sup>37</sup> is being conducted on techniques that could allow to remove situational information like background noises and anonymize the voice.

### Recommendations

106. From a user's perspective, the main purpose of processing their data is querying and receiving responses and/or triggering actions like playing music or turning on or off lights. After a query has been answered or a command executed, the personal data should be deleted unless the VVA designer or developer has a valid legal basis to retain them for a specific purpose.
107. Before considering anonymization as means for fulfilling the data storage limitation principle, VVA providers and developers should check the anonymization process renders the voice unidentifiable.
108. Configuration defaults should reflect these requirements by defaulting to an absolute minimum of stored user information. If these options are presented as part of a setup wizard, the default setting should reflect this, and all options should be presented as equal possibilities without visual discrimination.
109. When during the review process the VVA provider or developer detects a recording originated on a mistaken activation, the recording and all the associated data should be immediately deleted and not used for any purpose.

### 3.7 Security

110. To securely process personal data, VVAs should protect their confidentiality, integrity and availability. Apart from risks stemming from elements on the VVA ecosystem, using voice as communication means creates a new set of security risks.
111. VVAs are multiuser. They may allow for more than one registered user and anyone on their surroundings can issue commands and use their services. Any VVA service requiring confidentiality will involve some access control mechanism and user authentication. Without access control, anyone able to issue voice commands to the VVA could access, modify or delete any users' personal data it (e.g. ask for received messages, user's address or calendar events). Issuing voice commands to the VVA does not require being physically close to it since they can

---

<sup>37</sup> See, for example, VoicePrivacy (<https://www.voiceprivacychallenge.org>), an initiative to develop privacy preservation solutions for speech technology.

See also open-source voice anonymization tools developed by H2020 research and innovation project COMPRIZE: [https://gitlab.inria.fr/comprise/voice\\_transformation](https://gitlab.inria.fr/comprise/voice_transformation).

be manipulated, for example, via signal broadcasting<sup>38</sup> (e.g. radio or TV). Some of the known methods to remotely issue commands to VVAs like laser<sup>39</sup> or ultrasonic (inaudible) waves<sup>40</sup> are not even detectable by human senses.

112. User authentication can rely on one or more of the following factors: something you know (such as a password), something you have (such as a smart card) or something you are (such as a voice fingerprint). A closer look at these authentication factors in the VVA context shows that:
  - | Authentication using something the user knows is problematic. The secret that would allow users to prove their identity should be spoken aloud, exposing it to anyone in the surroundings. VVAs communication channel is the surrounding air, a channel type that cannot be fortified in the way traditional channels are (e.g. by limiting the access to the channel or encrypting its content).
  - | Authentication using something the user has would require the VVA service providers to create, distribute and manage “tokens” that could be used as proof of identity.
  - | Authentication using something the user is implies the use of biometric data for the purpose of uniquely identifying a natural person (see section 3.7 below).
113. VVA user accounts are associated to the devices in which the service is provided. Often the same account used to manage the VVA is used to manage other services. For example, owners of an Android mobile phone and a Google Home speaker can and most likely associate their Google account to both devices. Most VVAs do not require or offer an identification or authentication mechanism when a device providing a VVA service has just one user account.
114. When there is more than one user account associated with the device, some VVAs offer an optional basic access control in the form of PIN number with no real user authentication. Some other VVAs have the option to use voice fingerprint recognition as identification mechanism.
115. Although user identification or authentication might not be necessary to access all VVA services, it will definitely be for some. Without an identification or authentication mechanism, anyone could access other users’ data and modify or erase them at will. For example, anyone close to a smart speaker could delete other users’ playlists from the music streaming service, commands from the command history or contacts from the contact list.
116. Most VVAs blindly trust their local networks. Any compromised device in the same network could change the settings of the smart speaker or allow the installation of malware or to associate fake apps/skills to it without the user’s knowledge or agreement.<sup>41</sup>

---

<sup>38</sup> X. Yuan et al., "[All Your Alexa Are Belong to Us: A Remote Voice Control Attack against Echo](#)" 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, 2018, pp. 1-6, doi: 10.1109/GLOCOM.2018.8647762.

<sup>39</sup> See, for example, <https://lightcommands.com>

<sup>40</sup> See, for example, <https://surfingattack.github.io>

<sup>41</sup> See, for example, Deepak Kumar et al., *Skill Squatting Attacks on Amazon Alexa*, USENIX Security Symposium, August 2018, <https://www.usenix.org/conference/usenixsecurity18/presentation/kumar>

Security Research Labs, *Smart Spies: Alexa and Google Home expose users to vishing and eavesdropping*, November 2019, <https://srlabs.de/bites/smart-spies>

- 117. VVAs, like any other software, are subject to software vulnerabilities. However, due to the VVA market concentration<sup>42</sup> any vulnerability could affect millions of VVA users. If working as currently designed, VVAs do not send any information to the speech recognition cloud service until the wake-up expression is detected. However, software vulnerabilities could allow an attacker to bypass the VVA set-up and security measures. It could then be possible for example to get a copy of all data sent to the VVA cloud and forward it to a server controlled by the attacker.
- 118. Data lawfully processed or derived by VVAs allow building a fairly accurate profile of their users as VVA know or can infer the location, the relations and the interests of their users. VVAs are increasingly present in users' homes and smartphones. This circumstance increases the risk of mass surveillance and mass profiling. Consequently, the security measures to protect the data both in transit and at rest, in the devices and in the Cloud, should match those risks.
- 119. The increasing use of VVA in conjunction with not adequately balanced access rights by law enforcement authorities could induce a chilling effect that would undermine fundamental rights like freedom of speech.
- 120. Law enforcement authorities, both in<sup>43</sup> and out<sup>44</sup> of the EU, have already expressed their interest in accessing the voice snippets captured by VVAs. Access to data processed or derived by VVAs in the EU should comply with the existing EU data protection and privacy regulation framework. In case some Member States consider issuing specific legislation restricting the fundamental rights to privacy and data protection, such restrictions should always comply with the requirement set out in Article 23 of the GDPR<sup>45</sup>.
- 121. The human review of voice recordings and associated data to improve VVA service quality is a common practice among VVA providers. Due to the sensitive nature of the data that is processed by this human reviewers and the fact that this process is often subcontracted to a processors, it is of utmost relevance that adequate security measures are put in place.

## Recommendations

- 122. VVA designers and application developers should provide secure state-of-the-art authentication procedures to users.
- 123. Human reviewers should always receive the strictly necessary pseudonymised data. The legal agreements governing the review should expressly forbid any processing that could lead to the identification of the data subject.
- 124. If emergency calling is provided as a service through the VVA, a stable uptime<sup>46</sup> should be guaranteed.

## 3.8 Processing of special categories of data

- 125. As previously mentioned, VVAs have access to information of an intimate nature which can be protected under article 9 of the GDPR (see section 3.7.1), such as biometric data (see section

<sup>42</sup> The VVA market is currently shared among less than a dozen service providers.

<sup>43</sup> See, for example, <https://www.ft.com/content/ad765972-87a2-11e9-a028-86cea8523dc2>.

<sup>44</sup> See, for example, <https://cdt.org/insights/alexa-is-law-enforcement-listening>.

<sup>45</sup> See also EDPR, Guidelines 10/2020 on restrictions under Article 23 GDPR.

<sup>46</sup> The time a device or a service can be left unattended without crashing, or needing to be rebooted for administrative or maintenance purposes.

3.7.2). Therefore, VVA designers and developers must carefully identify in which cases the processing implies special categories of data.

### 3.8.1 General considerations when processing special categories of data

126. VVAs may process special categories of data in different circumstances:

- ) As part of their own services, for example when managing medical appointments in users' agendas.
- ) When acting as interface for third-party services, VVA providers process the content of the commands. Depending on the type of service requested by the user, VVA providers could process special categories of data. An example could be when a user issues commands to a VVA to use a third-party app used to keep track of her ovulation.<sup>47</sup>
- ) When voice data is used for the purpose of uniquely identify the user, as developed below.

### 3.8.2 Specific considerations when processing biometric data

127. Some VVA have the capability of uniquely identifying their users merely based on their voice. This process is known as voice model recognition. During the enrolment phase of voice recognition, the VVA processes a user's voice to create a voice model (or voiceprint). During its regular use, the VVA can calculate the voice model of any users and compare it to the enrolled models to uniquely identify the user who executed a command.

#### Example 11:

A group of users set up a VVA to use voice model recognition. After doing so, each of them enrol their voice models.

Later, a user requests the VVA access to the meetings in his or her agenda. Since access to the agenda requires user identification, the VVA extracts the model from the request's voice, calculates its voice model and checks if it matches an enrolled user and if that specific user has access to the agenda.

128. In the example above, the recognition of a the user's voice on the basis of a voice model amounts to the processing of special categories of personal data within the meaning of Article 9 GDPR (processing of biometric data for the purpose of uniquely identifying a natural person).<sup>48</sup> The processing of biometric data for the purpose of user identification as required in the example will require the explicit consent of the data subject(s) concerned (Article 9(2)(a) GDPR). Therefore, when obtaining users' consent, data controllers must comply with the conditions of Article 7 and as clarified in recital 32 of the GDPR and should offer an alternative identification method to biometrics, with regard to the free nature of consent.

129. When using voice data for biometric identification or authentication, data controllers are required to make transparent where biometric identification is used and how voiceprints

<sup>47</sup> See for example, a product available here: <https://www.amazon.com/Ethan-Fan-Ovulation-Period-Tracker/dp/B07CRLSHKY>

(biometric models) are stored and propagated across devices. To fulfil this transparency requirement, the EDPB recommends to provide the answers to the following questions:

- | Does the activation of voice identification on one device automatically activate this feature on all other devices running with the same account?
- | Does the activation of voice identification propagate through the VVA controller's infrastructure to devices owned by other users?
- | Where are biometric models generated, stored and matched?
- | Are biometric models accessible to VVA providers, developers or others?

130. When the registered user configures the VVAs to identify the voice of its users, the voice of non-registered and accidental users will also be processed for the purpose of uniquely identifying them.

131. Indeed, detecting the voice of the right speaker also involves comparing it with that of other people in the assistant's vicinity. In other words, the speaker recognition functionality implemented in voice assistants may require the voice biometrics of people speaking in the household to be recorded, to allow the user's voice characteristics to be distinguished from those of the person who wishes to be recognised. Biometric identification may therefore have the consequence of subjecting uninformed persons to biometric processing, by registering their model and comparing it with that of the user wishing to be recognised.

132. In order to avoid such collection of biometric data without the knowledge of the data subjects while allowing a user to be recognized by the assistant, solutions based on the user's data alone should be given priority. In concrete terms, this means that biometric recognition is only activated at each use at the user's initiative, and not by a permanent analysis of the voices heard by the assistant. For instance, a specific keyword or question to the persons present could be provided in order to obtain their consent to trigger biometric processing. For example, the user can say "identification" or the assistant can ask "do you wish to be identified" and wait for a positive response to activate biometric processing.

**Example 12:**

If the user wishes to set up biometric authentication for access to certain protected data such as his/her bank account, the voice assistant could activate speaker verification, when he/she launches the application only, and verify his/her identity in this way.

## Recommendations

133. Voice models should be generated, stored and matched exclusively on the local device, not in remote servers.
134. Due to the sensitiveness of the voiceprints, standards such as ISO/IEC 24745 and techniques of biometric model protection<sup>49</sup> should be thoroughly applied.

---

<sup>49</sup> See for example:

Jain, Anil & Nandakumar, Karthik & Nagar, Abhishek. (2008). "*Biometric Template Security*". EURASIP Journal on Advances in Signal Processing. 2008. 10.1155/2008/579416.

S. K. Jami, S. R. Chalamala and A. K. Jindal, "*Biometric Template Protection Through Adversarial Learning*" 2019 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 2019, pp. 1-6, doi: 10.1109/ICCE.2019.8661905.

135. If a VVA uses voice based biometric identification VVA providers should:
- ✓ Ensure that the identification is accurate enough to reliably associate personal data to the right data subjects.
  - ✓ Ensure that the accuracy is similar for all user groups by checking that there is no substantial bias towards different demographic groups.

### 3.9 Data minimization

136. Controllers should minimize the amount of data that is collected directly or indirectly and obtained by processing and analysis, e.g. not perform any analysis on the user's voice or other audible information to derive information about their mental state, possible disease or circumstances of their life.
137. Roll out settings by default that limit any data collecting and/or processing to a minimum required amount needed to provide the service.
138. Depending on the location, use context and microphone sensitivity, VVA could collect third parties' voice data as part of the background noise when collecting the users' voice. Even if background noise does not include voice data, it can still include situational data that could be processed to derive information about the subject (e.g. location).

### Recommendations

139. VVA designers should consider technologies deleting the background noise to avoid recording and processing background voices and situational information.

### 3.10 Accountability

140. For any processing that is based on consent, controllers are obliged to be able to prove the consent of data subjects according to Article 7 (1) GDPR. Voice data can be used for accountability (e.g. to prove consent). The retention obligation for such voice data would then be dictated by the accountability requirements of the relevant specific legislation.
141. When evaluating the need for a Data Protection Impact Assessment (DPIA), the EDPB set out criteria<sup>50</sup> to be used by data protection authorities in creating lists of processing operations that require a mandatory DPIA and provide examples of processing that are likely to require a DPIA. It is very likely that VVA services fall into the categories and conditions identified as needing a DPIA. This includes considering if the device may be observing monitoring or controlling data subjects or systematically monitoring at large scale as per Article 35(3)(c), use of "new technology", or the processing of sensitive data and data concerning vulnerable data subjects.
142. All data collection and processing activities must be documented in accordance with Article 30 GDPR. That includes all processing involving voice data.

---

<sup>50</sup> Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA), wp248, rev.01, endorsed by EDPB.

## Recommendations

143. If voice messages are to be used to inform users according to Article 13, the data controllers should publish such messages on their website so they are accessible to the users and the data protection authorities.

### 3.11 Data protection by design and by default

144. VVA providers and developers should consider the necessity of having a registered user for each of their functionalities. While it is clear that it is necessary to have a registered user to manage an agenda or an address book, it is not so clear that making a phone call or an Internet search requires the VVA to have a registered user.
145. By default, services which do not require an identified user should not associate any of the VVA identified users to the commands. A privacy and data protection friendly default VVA would only process users' data for executing users' requests and would store neither voice data nor a register of executed commands.
146. While some devices can only run one VVA, others can choose among different VVAs. VVA providers should develop industry standards enabling data portability in accordance with Article 20 of the GDPR.
147. Some VVA providers alleged their VVAs could not delete all users' data even when requested by the data subject. VVA providers should ensure that all users' data can be erased at the user's request in accordance with Article 17 of the GDPR.

## 4 MECHANISMS TO EXERCISE DATA SUBJECT RIGHTS

148. In compliance with the GDPR, data controllers providing VVA services must allow all users, registered and non-registered, to exercise their data subject rights.
149. VVA providers and developers should facilitate data subjects' control over their data during the entire processing period, in particular ease their right of access, rectification, erasure, their right to restrict the processing and, depending on the legal basis of the processing, their right to data portability and their right to object.
150. The data controller should provide information on the data subject's rights at the time when data subjects switch on a VVA and at the latest, at the time when the first user's voice request is processed.
151. Given that the main interaction means for VVAs is voice, VVA designers should ensure that users, registered or not, can exercise any data subject rights, using easy-to-follow voice commands. VVA designers, as well as app developers in case they are part of the solution, should at the end of the exercise process inform the user that his/her rights have been duly factored, by voice or by providing a writing notification to the user's mobile, account or any other mean chosen by the user.
152. At least, VVA designers and app developers, notably, should implement specific tools providing an effective and efficient way to exercise such rights. They should therefore propose for their devices, a way to exercise data subjects' rights as by providing the data subject with self-

service tools, as a profile management system<sup>51</sup>. This could facilitate an efficient and timely handling of data subject's rights and will enable the data controller to include the identification mechanism in the self-service tool.

153. In regards of the exercise of data subjects rights in case of multiple users, when a user, registered or not, exercises one of his or her rights, he or she should do so without prejudice to any other users' rights. All the users, registered and non-registered can exercise their rights as long as the data controller is still processing the data. Data controller should set up a process ensuring that data subject rights are exercised.

#### 4.1 Right to access

154. According to Article 12(1) GDPR, communication under Article 15 should be provided in writing, or by other means, including, where appropriate, by electronic means. As regards access to the personal data undergoing processing, Article 15(3) states that where the data subject makes the request by electronic means, and unless otherwise requested by the data subjects, the information should be provided in a commonly used electronic form. What could be considered as a commonly used electronic form should be based upon the reasonable expectations of the data subjects and not upon what format the data controller uses in its daily operations. The data subject should not be obliged to buy specific software or hardware in order to get access to the information.
155. On demand, data controllers should therefore send a copy of personal data, and audio data (including voice recordings and transcriptions) in particular, in a common format readable by the data subject.
156. When deciding about the type of format the information under Article 15 should be provided in, the data controller needs to keep in mind that the format should enable the information to be presented in a way that is both intelligible and easy accessible. Data controllers should also tailor the information to the specific situation of the data subject making the request.

##### Example 13:

A data controller providing a VVA service receives, from a user, both a request of access and a request for data portability. The data controller decides to provide the information under both Article 15 and Article 20 in a PDF file. In such a case, the data controller should not be considered to handle both requests in a correct manner. A PDF file technically fulfils the obligations on the data controller under Article 15, but does not fulfil the obligations on the data controller under Article 20.<sup>52</sup>

It should be noted that simply referring users to a history of their interactions with the voice assistant does not appear to enable the data controller to meet all its obligations under the right of access, as the accessible data generally represents only part of the information processed in the context of providing the service.

---

<sup>51</sup> Profile management system is understood as a place within the VVA system, where users may, anytime, store its preferences, set modification and change easily his/her privacy settings

<sup>52</sup> WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 18.

157. The right of access should not be used to counter / to get around the principles of minimisation and data retention.

#### 4.2 Right to rectification

158. To facilitate data rectification, users, registered or not, should be able to manage and update, at any time, their data by voice directly from the VVA device, as described above. Furthermore self-service tool should be implemented inside the device or an application in order to help them to rectify easily their personal data. Users should be notified by voice, or by writing of the update.
159. More generally, the right to rectification applies to any opinions and inferences<sup>53</sup> of the data controller, including profiling, and should consider the vast majority of data is highly subjective.<sup>54</sup>

#### 4.3 Right to erasure

160. Users, registered or not, should be able, at any time, by voice from the VVA device, or from a self-service tool integrated into any device associated to the VVA, to delete data concerning them. In this respect, the personal data can be deleted by a data subject as easily as it is submitted. Due to the inherent difficulties of anonymising voice data and the wide variety of personal data collected from, observed and inferred about the data subject,<sup>55</sup> in this context the right to erasure could be hardly accommodated by anonymising personal datasets. As the GDPR is technology neutral and technology evolves rapidly, it will nevertheless not be excluded that right to erasure may be made effective through anonymization.
161. In some cases, without a third party screen or the possibility of displaying data stored (e.g. a mobile application or a tabular device), it is difficult to have a preview of the recorded tracks, to judge the relevance of the suggestions. A dashboard (or an application) widely accessible to users in order to ease its use should be supplied with the voice assistant to delete the history of the requests asked and customize the tool according to user's needs.<sup>56</sup>
162. For any data processing and, in particular, when registered data subjects consent to the voice recordings to be transcribed and used by the provider for the improvement of its services, VVA providers should, on demand of the user, be able to delete the initial voice recording as well as any related transcription of the personal data.
163. The data controller should ensure that no more processing may occur, after the exercise of the right of erasure. In regards to previous actions, the right to erasure may meet some legal and technical limits, notably.

---

<sup>53</sup> The fact that opinions and inferences can qualify as personal data has been confirmed by the CJEU, which noted that the term 'any information' in the definition of personal data includes information that is 'not only objective but also subjective, in the form of opinions and assessments, provided that it 'relates' to the data subject' - Case C-434/16 *Peter Nowak v Data Protection Commissioner* ECLI:EU:C:2017:994 [34].

<sup>54</sup> Getting Data Subject Rights Right, A submission to the EDPB from data protection academics, November 2019.

<sup>55</sup> Article 29 Working Party Opinion 05/2014 on Anonymisation Techniques, adopted on 10 April 2014.

<sup>56</sup> "Assistants vocaux et enceintes connectées, l'impact de la voix sur l'offre et les usages culturels et médias", the French "Conseil Supérieur de l'Audiovisuel", May 2019.

**Example 14:**

If prior to the deletion request, a user made an online purchase by means of his/her VVA, the VVA provider may delete the voice recording relating to the online purchase and ensure no more future further use. However, the purchase will still be effective as well as the vocal order or the written transcription processed by the e-commerce website (here the exemption is based of legal obligation of the e-commerce website).

In the same vein, if prior to the deletion request, the user added a specific song to his/her playlist, by means of his/her VVA, the VVA providers will be able to delete the oral request, but not the past consequences of such request (the erasure will not impact the user's playlist).

164. Based on the above, in case the same personal data is processed for different processing purposes, data controllers should interpret erasure requests as a clear signal to stop processing of the data for all purposes that are not legally exempted.

In accordance with the conditions set out in Article 21(1) of the GDPR, data processed on the basis of legitimate interests of the VVA providers should not be an exemption to the right of erasure, in particular, because data subjects do not reasonably expect further processing of their personal data.

#### 4.4 Right to data portability

165. The data processing made by the VVA providers falls under the scope of data portability, as processing operations are mainly based, on the data subject's consent (under Article 6(1)(a), or under Article 9(2)(a) when it comes to special categories of personal data) or, on a contract to which the data subject is a party under Article 6(1)(b).
166. In practice, the right to data portability should facilitate switching between different VVA providers. VVAs operating in a digital environment in particular and data subject's voice being recorded in an application or a platform, the right to data portability should be granted for all personal data provided by the data subject. Furthermore, the data controller should offer users the possibility of directly retrieving their personal data from their user area, as a self-service tool. The users should also be able to exercise this right through voice command.
167. VVA providers and developers should give to the data subjects an extensive control over the personal data concerning him or her, in order to allow them to transfer personal data from a VVA provider to another. Data subjects should, therefore, receive his/her personal data provided to the data controller, in a structured, commonly used and machine-readable format as well as from means<sup>57</sup> that contribute to answer data portability requests (such as download

---

<sup>57</sup> See as an illustration, the reasoning of the Article 29 Working Party in the Guidelines on the right to data portability - endorsed by the EDPB, p. 16:

*"On a technical level, data controllers should explore and assess two different and complimentary paths for making portable data available to the data subjects or to other data controllers:*

*- a direct transmission of the overall dataset of portable data (or several extracts of parts of the global dataset);*  
*- an automated tool that allows extraction of relevant data.*

*The second way may be preferred by data controllers in cases involving of complex and large data sets, as it allows for the extraction of any part of the data-set that is relevant for the data subject in the context of his or her request, may help minimizing risk, and possibly allows for use of data synchronization mechanisms (e.g. in the context of a regular communication between data controllers). It may be a better way to ensure compliance for the "new" data controller, and would constitute good practice in the reduction of privacy risks on the part of the initial data controller".*

tools and Application Programming Interfaces)<sup>58</sup>. As stated in the Guidelines on the right to data portability, in case of large or complex personal data collection, that could be the case here, the data controller should provide an overview “*in a concise, transparent, intelligible and easily accessible form, using clear and plain language*” (see Article 12(1) of the GDPR) in such a way that data subjects should always have clear information of what data to download or transmit to another data controller in relation to a given purpose. For example, data subjects should be in a position to use software applications to easily identify, recognize and process specific data from it.

168. This right should allow the user to retrieve for his/her personal use, the data that he/she has communicated by means of his/her voice (e.g. the history of voice interactions) and within the framework of the creation of his/her user account (e.g.: name and first name), notably.
169. For the full application of this data subjects’ right in a context of one digital single market, VVA designers and app developers, notably, should develop common machine-readable formats that ease interoperability of the data format between VVA systems<sup>59</sup>, including the standard formats for voice data. Technologies should be structured in order to ensure that personal data, including voice data, processed are easily and fully reusable by the new controller<sup>60</sup>.
170. In regards to the format, VVA providers should provide personal data using commonly used open formats (e.g. mp3, wav, csv, gsm, etc.) along with suitable metadata used in order to accurately describe the meaning of exchanged information.<sup>61</sup>

## 5 ANNEX: AUTOMATIC SPEECH RECOGNITION, SPEECH SYNTHESIS AND NATURAL LANGUAGE PROCESSING

171. Following the theoretical foundations of signal processing, notably Claude Shannon’s information and sampling theories, automatic speech processing has become a fundamental component of engineering sciences. At the crossroads of physics (acoustics, wave propagation), applied mathematics (modelling, statistics), computer science (algorithms, learning techniques) and human sciences (perception, reasoning), speech processing has rapidly been broken down into numerous subjects of study: speaker identification and verification, automatic speech recognition, voice synthesis, emotion detection, etc. Over the last fifteen years or so, the discipline as a whole has made very significant progress, with various factors contributing to this: improved methods, a significant increase in computing capacities and greater volumes of data available.

---

<sup>58</sup> In this respect: Article 29 Working Party Guidelines on the right to data portability - endorsed by the EDPB, p. 1.

<sup>59</sup> In this respect: recital (68) of the GDPR; WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 17.

<sup>60</sup> “*In this respect, recital 68 encourages data controllers to develop interoperable formats that enable data portability but without creating an obligation for controllers to adopt or maintain processing systems which are technically compatible. The GDPR does, however, prohibit controllers from establishing barriers to the transmission*” - WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 5.

<sup>61</sup> EDPB strongly encourages cooperation between industry stakeholders and trade associations to work together on a common set of interoperable standards and formats to deliver the requirements of the right to data portability.

## 5.1 Automatic Speech Recognition (ASR)

172. The automatic speech recognition (also known as speech to text) used to involve three distinct stages aimed at: 1) determine which phonemes were said using an acoustic model; 2) determine which words were said using a phonetic dictionary; 3) transcribe the sequence of words (sentence) most likely to have been said using a language model. Today, with the progress made possible by deep learning (a machine learning technique), many systems offer "end to end" automatic speech recognition. This avoids the need to go through the complex training of three different models while offering better performance in terms of results and processing time. Almost all major digital players now offer their own ASR implementations that can be easily used by API systems, but open-source systems also exist (DeepSpeech<sup>62</sup> or Kaldi<sup>63</sup> for example).

## 5.2 Natural Language Processing (NLP)

173. Natural Language Processing is a multidisciplinary field involving linguistics, computer science and artificial intelligence, which aims to create natural language processing tools for a variety of applications. The fields of research and applications are numerous: syntactic analysis, machine translation, automatic text generation and summarization, spell checking, question answering systems, text mining, named entity recognition, sentiment analysis, etc. Concretely, NLP's goal is to give computers the ability to read, understand and derive meaning from human languages. The development of NLP applications is challenging because computer tools traditionally require humans to interact with them in a programming language that is formal, meaning precise, unambiguous and highly structured. Human speech, however, is not always precise. It is often ambiguous and the linguistic structure can depend on many complex variables, including slang, regional dialects and social context.

174. Syntax and semantic analysis are two main techniques used with NLP. Syntax is the arrangement of words in a sentence to make grammatical sense. NLP uses syntax to assess meaning from a language based on grammatical rules. Syntax techniques used include parsing (grammatical analysis for a sentence), word segmentation (which divides a large piece of text to units), sentence breaking (which places sentence boundaries in large texts), morphological segmentation (which divides words into groups) and stemming (which divides words with inflection in them to root forms). Semantics involves the use and meaning behind words. NLP applies algorithms to understand the meaning and structure of sentences. Techniques that NLP uses with semantics include word sense disambiguation (which derives meaning of a word based on context), named entity recognition (which determines words that can be categorized into groups), and natural language generation (which will use a database to determine semantics behind words). While earlier approaches to NLP involved rules-based approaches, where simple machine learning algorithms were told what words and phrases to look for in text and given specific responses when those phrases appeared, current approaches to NLP are based on deep learning, a type of AI that examines and uses patterns in data to improve a program's understanding.

## 5.3 Speech Synthesis

175. Speech synthesis is the artificial production of human speech. Speech synthesis has mainly been implemented by concatenation of vocal units that are stored in a database. This technique consists in selecting, from all the recordings of an actor previously transcribed into

---

<sup>62</sup> <https://github.com/mozilla/DeepSpeech>

<sup>63</sup> <https://github.com/kaldi-asr/kaldi>

phonemes, syllables and words, the bricks of sound that correspond to the words that one wishes to have pronounced by the VVA and to assemble them one after the other to form an intelligible sentence with natural diction. Alternatively, a speech synthesizer can incorporate a model of the vocal tract and other human voice characteristics in order to model the parameters of a voice such as intonation, rhythm, and timbre, by generative statistical models (such as WaveNet<sup>64</sup>, Tacotron<sup>65</sup> or DeepVoice<sup>66</sup>) and to create a completely synthetic voice output.

---

<sup>64</sup> Aäron van den Oord et Sander Dieleman, *WaveNet: A generative model for raw audio*, Deepmind blog, september 2016, <https://deepmind.com/blog/article/wavenet-generative-model-raw-audio>

<sup>65</sup> Yuxuan Wang, *Expressive Speech Synthesis with Tacotron*, Google AI blog, March 2018, <https://ai.googleblog.com/2018/03/expressive-speech-synthesis-with.html>

<sup>66</sup> Deep Voice 3: 2000-Speaker Neural Text-to-Speech, Baidu Research blog, October 2017 <http://research.baidu.com/Blog/index-view?id=91>

# Guidelines



**Guidelines 03/2021 on the application of Article 65(1)(a)  
GDPR**

**Version 2.1**

**Adopted on 24 May 2023**

## Version history

Version 1.0	13 April 2021	Adoption of the Guidelines for public consultation
Version 2.0	24 May 2023	Adoption of the Guidelines after public consultation
Version 2.1	15 July 2024	Editorial corrections

## **Executive summary**

Article 65(1)(a) GDPR is a dispute resolution mechanism meant to ensure the correct and consistent application of the GDPR in cases involving cross-border processing of personal data. It aims to resolve conflicting views among the LSA(s) and CSA(s) on the merits of the case, in particular whether there is an infringement of the GDPR or not, in order to ensure the correct and consistent application of the GDPR in individual cases. These Guidelines clarify the application of the dispute resolution procedure under Article 65(1)(a) GDPR.

Article 65(1)(a) GDPR requires the EDPB issues a binding decision whenever a Lead Supervisory Authority (LSA) issues a draft decision and receives objections from Concerned Supervisory Authorities (CSAs) that either it does not follow or it deems to be not relevant and reasoned.

These Guidelines clarify the applicable legal framework and main stages of the procedure, in accordance with the relevant provisions of the Charter of Fundamental Rights of the European Union, the GDPR and EDPB Rules of Procedure. The Guidelines also clarify the competence of the EDPB when adopting a legally binding decision on the basis of Article 65(1)(a) GDPR. In accordance with Article 65(1)(a) GDPR, the EDPB binding decision shall concern all the matters which are the subject of the relevant and reasoned objection. Consequently, the EDPB will first assess whether the objection(s) raised meet the “relevant and reasoned” standard set in Article 4(24) GDPR. Only for the objections meeting this threshold, the EDPB will take a position on the merits of the substantial issues raised. The Guidelines analyse examples of objections signalling disagreements between the LSA and CSA(s) on specific matters and clarify the EDPB’s competence in each case.

The Guidelines also clarify the applicable procedural safeguards and remedies, in accordance with the relevant provisions of the Charter of Fundamental Rights of the European Union, the GDPR and EDPB Rules of Procedure. In particular, these Guidelines address the right to be heard, the right of access to the file, the duty for the EDPB to provide reasoning for its decisions, as well as a description of the available judicial remedies.

These Guidelines do not concern dispute resolution by the EDPB in cases where: (1) there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment (Article 65(1)(b) GDPR); or (2) a competent supervisory authority does not request the opinion of the Board in the cases referred to in Article 64(1), or does not follow the opinion of the Board issued under Article 64 (Article 65(1)(c) GDPR).

## Table of contents

1	Introduction and scope.....	6
2	Legal framework and Rules of Procedure.....	7
2.1	Right to good administration.....	7
2.2	GDPR .....	8
2.3	EDPB Rules of procedure (RoP) .....	8
3	Main stages of the procedure (overview) .....	8
3.1	Conditions for adopting a binding decision .....	8
3.2	Assessment of the completeness of the file .....	9
3.3	Establishment of deadline(s) .....	12
3.3.1	Calculation .....	12
3.3.2	Decision to extend by one month .....	13
3.3.3	Extension by two weeks .....	13
3.4	Preparation of the draft EDPB binding decision.....	13
3.5	Adoption of the EDPB binding decision.....	14
3.6	Notification to the supervisory authorities concerned .....	14
3.7	Final Decision of the supervisory authority(ies) .....	15
3.7.1	“On the basis of” .....	15
3.7.2	Decision(s) by LSA and/or CSA.....	16
3.7.3	Information to the EDPB.....	16
3.8	Publication of the EDPB binding decision.....	16
4	Competence of the EDPB.....	17
4.1	Assessment of whether the objections are relevant and reasoned .....	18
4.2	Matters subject of the relevant and reasoned objection .....	19
4.2.1	Existence of a given infringement of the GDPR.....	19
4.2.2	Additional or alternative infringements of the GDPR .....	19
4.2.3	Gaps in the draft decision justifying the need for further investigation by the LSA.....	20
4.2.4	Insufficient factual information or reasoning.....	21
4.2.5	Procedural aspects.....	22
4.2.6	Action envisaged.....	23
5	The Right to be heard .....	23
5.1	Applicability .....	23
5.2	Purpose .....	25
5.3	Timing .....	25
5.3.1	At national level and prior to referral to the EDPB .....	25

5.3.2	During the assessment of completeness of the file .....	25
6	Access to the file.....	26
7	The duty to give reasons.....	28
8	Judicial remedies .....	29
8.1	Supervisory authorities.....	30
8.2	Controller, processor, complainant, or other entity .....	31

## 1 INTRODUCTION AND SCOPE

1. Article 65(1)(a) GDPR requires the EDPB to issue a legally binding decision whenever a Lead Supervisory Authority (LSA) issues a draft decision within the meaning of Article 60(3) GDPR and decides not to follow a relevant and reasoned objection expressed by a Concerned Supervisory Authority (CSA) or is of the opinion that the objection is not relevant or reasoned<sup>1</sup>.
2. Article 65(1)(a) GDPR is a **dispute resolution** mechanism meant to ensure the correct and consistent application of the GDPR in cases involving cross-border processing of personal data<sup>2</sup>. It aims to resolve conflicting views among the LSA(s) and CSA(s) on the merits of the case, in particular whether there is an infringement of the GDPR or not, in order to ensure the correct and consistent application of the GDPR in individual cases<sup>3</sup>.
3. Under the so-called ‘one-stop-shop mechanism’, which applies to cross-border processing of personal data, the LSA acts as the sole interlocutor for the controller or processor for the processing at issue<sup>4</sup>. The LSA is responsible for carrying out the necessary investigations, communicating the relevant information to all CSAs and preparing a draft decision<sup>5</sup>. Prior to the adoption of the draft decision, the LSA is required to cooperate with the CSAs in an endeavour to reach consensus and the LSA and CSAs to exchange all relevant information<sup>6</sup>.
4. Once a draft decision has been prepared, the LSA shall submit this draft decision to all CSAs for their opinion and take due account of their views<sup>7</sup>. Within four weeks after having been consulted, a CSA can express a “relevant and reasoned objection” to the draft decision<sup>8</sup>. When no CSA objects, the LSA may proceed to adopt the decision. If any CSA expresses an objection, the LSA must decide whether it will follow the relevant and reasoned objection or is of the opinion that the objection is not relevant or reasoned. If the LSA does not intend to follow the objection(s) or considers the objection(s) are not relevant and reasoned, the LSA is obliged to refer the case to the EDPB for dispute resolution<sup>9</sup>.

---

<sup>1</sup> On the concept of relevant and reasoned objection see European Data Protection Board, Guidelines 9/2020 on relevant and reasoned objection under Regulation 2016/679, Version 2.0, 9 March 2021 (hereafter, “RRO Guidelines”), [https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_guidelines\\_202009\\_rro\\_final\\_en.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202009_rro_final_en.pdf).

<sup>2</sup> The cooperation and consistency mechanism is applicable to ‘individual cases’ regardless of whether the case concerns a complaint or ex officio inquiry/investigation.

<sup>3</sup> Recital (136) and Article 65(1)(a) GDPR.

<sup>4</sup> Article 56(6) GDPR. In cases involving data subject complaint(s), each CSA acts as the main point of contact for the data subject(s) in the territory of its Member State. See Article 60(7)-(9), Article 65(6) and article 77(2) GDPR. See also Recitals (130) and (141) GDPR.

<sup>5</sup> See Article 60(3) GDPR. In accordance with Article 60(2) GDPR, the LSA may request at any time the other CSA to provide mutual assistance pursuant to Article 61 and may conduct joint operations pursuant to Article 62 GDPR.

<sup>6</sup> This duty of cooperation applies to every stage of the procedure, starting with the inception of the case and extending to the whole decision-making process, see Article 60(1) GDPR and RRO Guidelines, paragraph 1. As part of the cooperation procedure, the LSA and CSAs are also required to exchange all relevant information with each other (Article 60(1) GDPR).

<sup>7</sup> Article 60(3) GDPR.

<sup>8</sup> Article 60(4) GDPR.

<sup>9</sup> Articles 60(4), 63 and 65(1)(a) GDPR. If the LSA intends to follow the objection(s) that are deemed relevant and reasoned, it shall submit a revised draft decision to all the CSAs. The CSAs then have a period of two weeks

5. The EDPB will then act as a dispute resolution body and adopt a **legally binding decision**. The LSA, and in some situations the CSA with which the complaint was lodged<sup>10</sup>, must adopt its final decision on the basis of the EDPB decision. The final decision of the competent supervisory authority will be addressed to the controller or processor and, where relevant, to the complainant.
6. These Guidelines clarify the application of Article 65(1)(a) GDPR. In particular, they clarify the application of the relevant provisions of the GDPR and Rules of Procedure, delineate the **main stages** of the procedure and clarify the **competence of the EDPB** when adopting a legally binding decision on the basis of Article 65(1)(a) GDPR. The Guidelines also include a description of the applicable **procedural safeguards and remedies**.
7. The present Guidelines do not concern dispute resolution by the EDPB in cases where:
  - there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment (Article 65(1)(b) GDPR);
  - a competent supervisory authority does not request the opinion of the Board in the cases referred to in Article 64(1), or does not follow the opinion of the Board issued under Article 64 (Article 65(1)(c) GDPR).

## 2 LEGAL FRAMEWORK AND RULES OF PROCEDURE

### 2.1 Right to good administration

8. The EDPB is subject to the Charter of fundamental rights of the European Union (CFEU), including Article 41 (right to good administration). This is also reflected in Article 11(1) EDPB Rules of Procedure<sup>11</sup>, which confirms that the EDPB must respect the right to good administration as set out by Article 41 CFEU.
9. Article 41 CFEU grants every person the right to have his or her affairs handled **impartially, fairly and within a reasonable time** by the institutions, bodies, offices and agencies of the Union. This includes the right of every person:
  - **to be heard** before any individual measure, which would affect him or her adversely is taken; and
  - **to have access** to his or her file, while respecting the legitimate interests of confidentiality and of professional and business secrecy.

The right to good administration also includes the obligation of the administration to **give reasons** for its decisions.

---

during which they can express their relevant and reasoned objections to the revised draft decision (Article 60(5) GDPR). See also RRO GLS, paragraphs 2-3.

<sup>10</sup> This will apply in particular if the complaint is totally or partially dismissed (Article 60 (8)-(9) GDPR). See further at paragraph 51 and following.

<sup>11</sup> EDPB Rules of Procedure, adopted on 25 May 2018, as last modified and adopted on 8 October 2020, available at [https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_rop\\_version\\_7\\_adopted\\_20201008\\_en.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_rop_version_7_adopted_20201008_en.pdf) (hereafter 'RoP').

## 2.2 GDPR

10. Article 65(1) GDPR identifies three different situations in which the EDPB acts as a dispute resolution body. The main rules applicable to the dispute resolution procedures are set out in Article 65(2)-(6) GDPR.
11. In case of a dispute resolution on the basis of Article 65(1)(a) GDPR, regard must also be given to Article 60 GDPR, which applies to the cooperation between the LSA and CSA in individual cases involving cross-border processing and specifies in which cases the LSA submit the matter to the EDPB for dispute resolution. While these Guidelines focus primarily on the application of Article 65(1)(a) GDPR, reference will also be made to the provisions of Article 60 GDPR insofar as they are relevant to clarify the main stages of the procedure and competence of the EDPB under Article 65(1)(a) GDPR<sup>12</sup>.

## 2.3 EDPB Rules of procedure (RoP)

12. Article 11 RoP further clarifies the rules applicable in cases where the EDPB is called upon to take a binding decision, including in the context of the dispute resolution procedure. Article 11(2) RoP contains rules that apply specifically to the dispute resolution procedure of Article 65(1)(a) GDPR.
13. While not the focus of these Guidelines, regard will also be had to Article 22 (Voting), Article 32 (Access to documents), Article 33 (Confidentiality of discussions) and Article 40 (Calculation of time limits) of the RoP, as appropriate.

# 3 MAIN STAGES OF THE PROCEDURE (OVERVIEW)

## 3.1 Conditions for adopting a binding decision

14. The general conditions for the adoption of a binding decision by the EDPB are set forth in Article 60(4)-(5) and Article 65(1)(a) GDPR.
15. The EDPB shall be competent to issue binding decisions on the basis of Article 65(1)(a) GDPR when the following conditions are met:
  - the submission of a draft decision within the meaning of Article 60(3) by the LSA to the CSAs;
  - at least one CSA has raised (one or more) objection(s) to the (revised) draft decision of the LSA within the deadline provided by Article 60(4)-(5) GDPR; and
  - the LSA has decided to not follow the objection(s) on the draft decision or rejected it (them) as not relevant or reasoned.
16. When these conditions are met, the EDPB shall be competent to adopt a binding decision on the basis of Article 65(1)(a) GDPR, which shall concern all the matters which are the subject of the relevant and reasoned objection(s), in particular whether there is an infringement of the GDPR<sup>13</sup>.
17. A mere “comment” expressed by a CSA in relation to a draft decision does not amount to an objection within the meaning of Article 4(24) GDPR. The existence of comments shall therefore not give rise to

---

<sup>12</sup> For additional guidance regarding Article 60 GDPR, see Guidelines 02/2022 on the application of Article 60 GDPR, 14 March 2022, available at [https://edpb.europa.eu/system/files/2022-03/guidelines\\_202202\\_on\\_the\\_application\\_of\\_article\\_60\\_gdpr\\_en.pdf](https://edpb.europa.eu/system/files/2022-03/guidelines_202202_on_the_application_of_article_60_gdpr_en.pdf).

<sup>13</sup> See Section 4 for further details concerning the competence of the EDPB in accordance with Article 65(1)(a) GDPR.

the obligation to trigger the Article 65(1)(a) procedure if the LSA decides not to give any effect to the comment. Moreover, any comment expressed does not constitute as such a matter to be decided by the EDPB as part of its binding decision. The LSA is required, however, to take due account of the views expressed by all CSAs<sup>14</sup> and, in cases where the conditions of Article 56(2) are met, take utmost account of the views expressed by the CSA with whom the complaint has been lodged when preparing the draft decision and take due account of the views expressed by all CSAs<sup>15</sup>.

### 3.2 Assessment of the completeness of the file

18. Article 11(2) RoP provides that the Chair and the LSA are responsible for deciding whether the file is complete<sup>16</sup>. The assessment of the completeness of the file is an important step in the procedure, designed to ensure that all conditions for adopting a binding decision are met and that the EDPB has all the information necessary for doing so<sup>17</sup>. The assessment of completeness of the file also serves as the starting point for the legal deadlines mentioned in Article 65(2)-(3) GDPR<sup>18</sup>. Finally, the assessment of completeness of the file also seeks to ensure compliance with the right to be heard contained in Article 41 CFEU.
19. When submitting the matter to the EDPB for dispute resolution, the LSA shall include:
  - a) the **draft decision or revised draft decision** subject to the objection(s);
  - b) a **summary** of the relevant facts and grounds;
  - c) the **objection(s) made** by the supervisory authority(/-ies) concerned in accordance with Article 60 (4) (and where relevant Article 60(5) GDPR);
  - d) an **indication** as to whether the LSA **does not follow** the relevant and reasoned objection or is of the opinion that the objection is **not relevant or reasoned**;
  - e) **documentation proving the timing and format of the provision of the (revised) draft decision and of the objection(s)** by the concerned supervisory authority (/ -ies)<sup>19</sup>; and
  - f) in accordance with Article 41 of the European Charter on Fundamental Rights, the **written observations the LSA collected from the persons that might be adversely affected by the Board's decision**, together with confirmation and evidence of which documents submitted to the Board were provided to them when they were invited to **exercise their right to be heard** or a clear identification of the elements for which it is not the case<sup>20</sup>.
20. The wording of Article 60(4) GDPR and Article 11(2) RoP makes clear that the LSA is responsible for ensuring that the file is complete and submitting all relevant information to the EDPB. Where necessary, however, the Secretariat may request from the LSA and/or CSAs additional information

---

<sup>14</sup> Article 60(3) GDPR.

<sup>15</sup> Article 56(4) and Article 60(1) GDPR.

<sup>16</sup> The Secretariat carries out the analysis on the completeness of the file on behalf of the Chair.

<sup>17</sup> When necessary, the documents submitted by the competent authority will be translated into English by the EDPB Secretariat.

<sup>18</sup> See Article 11(4) RoP and see further Section 3.3.

<sup>19</sup> The aim of providing this information is to allow the Secretariat to verify the objection has been provided in writing and within the legal deadline. The timing and format of the provision of the (revised) draft decision and of the objection(s) can be proven, for example, via the relevant and reasoned objections report from the information and communication system mentioned in Article 17 of the RoP.

<sup>20</sup> Article 11(2) RoP. See also section 5.

within a specific timeframe<sup>21</sup>. The ability to request additional information should be interpreted in light of the objective of ensuring that the EDPB is provided with all information necessary to take a binding decision concerning all the matters which are the subject of the relevant and reasoned objection(s), in particular whether there is an infringement of the GDPR.

**Example 1:**

A draft decision includes several references to internal documentation of the controller. Even though the LSA's (disputed) finding of an infringement is evidenced in its draft decision with reference to the contents of this documentation, the LSA does not include a copy thereof when submitting the matter to the EDPB for dispute resolution. The Secretariat may request the LSA to provide a copy of the documentation that is referenced within a specific timeframe if needed to help decide the subject matter of the relevant and reasoned objection(s).

The ability to request additional information at a later stage does not diminish the responsibility of the LSA to provide all relevant information from the outset when submitting the matter to the EDPB. As the responsibility for ensuring that the file is complete lies with the LSA, the requesting of additional information from the LSA and/or CSA should in principle only be necessary in exceptional circumstances. Moreover, as the LSA and CSA are obliged to exchange all relevant information in the course of the cooperation procedure, the relevant information should already have been provided to CSAs prior to launching the dispute resolution procedure. If all information necessary to take a binding decision on the objections raised is also transmitted by the LSA when referring the subject matter to the EDPB, it will not be necessary for the Secretariat to request additional information before declaring the file complete.

21. It should be noted that a request for additional information merely seeks to ensure the completeness of the file. It does *not* imply any judgement regarding the merit of the objections raised, nor does it alter in any way the subject matter referred to the EDPB. Once the file is deemed complete and the subject matter is referred to the EDPB, in exceptional circumstances, additional information may also be requested at a later stage in the procedure (i.e. once the subject matter has been referred to the Board) if necessary to remedy any omissions. This will be subject to a decision by the EDPB<sup>22</sup>.
22. When necessary, the documents submitted by the LSA and/or CSA will be translated into English by the Secretariat<sup>23</sup>. The translation may also be limited to the specific parts which are likely to be relevant to help decide the subject matter of the relevant and reasoned objection(s). The LSA and/or CSA will have to agree on the translation<sup>24</sup>.

**Example 2:**

In its draft decision, the LSA concludes that only one of the infringements of the GDPR alleged by the complainant materialised. The CSA considers in its relevant and reasoned objection that the other infringements alleged by the complainant were also committed while the draft decision does not fully explain the factual elements necessary to conclude the infringements did not occur. Therefore, the Secretariat requests the LSA to provide a copy of the necessary parts of the investigation report within

---

<sup>21</sup> Article 11(2) RoP.

<sup>22</sup> Article 11(2) RoP provides that in exceptional circumstances, the EDPB can decide to consider further documents it deems necessary. As a result, the additional information may be requested by the Secretariat/Chair but the EDPB will have to decide if it will consider or not the additional info received.

<sup>23</sup> The competent authority must express its agreement with the translation provided (Article 11(2) RoP).

<sup>24</sup> Article 11(2) RoP.

a specific timeframe<sup>25</sup>. If the translation of these parts is necessary, it will be translated into English by the Secretariat and the LSA will have to agree on the translation.

23. Once the Chair and the LSA have decided that the file is complete (and the competent supervisory authority agreed on any required English translations), the Secretariat on behalf of the Chair will refer the subject-matter to the members of the EDPB without undue delay<sup>26</sup>.
24. If the LSA fails to provide the information listed above within the set timeframe<sup>27</sup>, the Chair will ask the Secretariat to refer the subject-matter to the EDPB. The EDPB will then assess, on a case-by-case basis, whether it can proceed to adopt its decision on the basis of the information already provided, or whether it is necessary to first obtain the information requested (e.g., confirmation and evidence of which documents submitted to the Board were provided to them when they were invited to exercise their right to be heard or a clear identification of the elements for which it is not the case) before adopting a decision.

*Relationship with the right to be heard*

25. The assessment of completeness of the file also seeks to ensure compliance with the right to be heard contained in Article 41 CFEU. Article 11(2) RoP provides that the EDPB shall take into account *only* the documents which were provided by the LSA and the other CSA(s) before the matter is referred to the Board. Any person who might be adversely affected should therefore in principle already have been invited to exercise their right to be heard<sup>28</sup>. Where necessary, the Board will take further actions ensuring the right to be heard of the affected persons in relation to the elements within the documents that are part of the file that will be considered by the EDPB in making its decision<sup>29</sup>.
26. Once the file has been declared complete, LSA and CSA(s) are in principle not able to submit any additional information concerning the subject matter of the dispute (unless requested by the Secretariat with a view of remedying an omission in accordance with Article 11(2) RoP<sup>30</sup>). Only in exceptional circumstances can the Board decide to consider further documents that it deems necessary. For example, the LSA cannot introduce new elements of fact supporting its decision not to follow one or more objections which were not previously communicated before the matter was referred to the EDPB<sup>31</sup>. Moreover, all information relevant to the assessment of the objections raised should already be exchanged between the LSA and CSA prior to the initiation of the Article 65(1)(a) procedure in an endeavour to reach consensus (as in doing so it may also help avoid the need for trigger the dispute resolution mechanism).

---

<sup>25</sup> Article 11(2) RoP.

<sup>26</sup> Article 11(2) RoP.

<sup>27</sup> Such a time-frame should be decided on a case-by-case basis, taking into account the nature and volume of the documents requested. The Secretariat should consult with the LSA (or where applicable, CSA) to seek their views as to what constitutes an appropriate timeframe.

<sup>28</sup> See in particular Article 11(2) RoP: “[ ...] together with confirmation and evidence of which documents submitted to the Board were provided to them when they were invited to exercise their right to be heard or a clear identification of the elements for which it is not the case.”

<sup>29</sup> See Section 5 for additional information regarding the exercise of the right to be heard.

<sup>30</sup> See paragraph 20 above.

<sup>31</sup> Indeed, the wording of Article 11(2)d RoP confirms that when launching the procedure, the LSA should give an “indication” as to whether it does not follow the relevant and reasoned objection or is of the opinion that the objection is not relevant or reasoned (i.e. simply an indication as to whether it follows or not the objections). As a result, no new elements may be submitted going beyond those of which the CSAs were informed prior to the submission to the Board.

27. Once the file has been declared complete and the subject matter has been referred to the EDPB, the EDPB must issue a binding decision in relation to each objection raised, unless the CSA who raised a particular objection decides to withdraw it. As the withdrawal of the objection signifies the end of the dispute between the LSA and CSA, it is no longer necessary for the EDPB to resolve the matter<sup>32</sup>. Similarly, the LSA may be able to withdraw a referral to the EDPB on the basis of Article 60(4) GDPR in cases where it later decides that it would like to follow each of the objections raised. The withdrawal of either an objection or referral should occur only in very exceptional cases, however, as the obligation for LSA and CSAs to seek consensus under Article 60 GDPR requires that the dispute resolution mechanism will only be triggered in cases of persistent disagreement and where reaching consensus was not possible.

### 3.3 Establishment of deadline(s)

28. The default legal deadline for the EDPB to adopt a binding decision is one month after the Chair and the competent supervisory authority have decided that the file is complete<sup>33</sup>. The deadline may be extended by a further month on account of the complexity of the subject-matter<sup>34</sup>. If the EDPB has not been able to adopt a decision, upon expiry of such an extension, it shall do so within two weeks following the expiration of the extension<sup>35</sup>.

#### 3.3.1 Calculation

29. The calculation of the deadline for the adoption of the binding decision must be done on the basis of Regulation 1182/71<sup>36</sup>. According to Article 3(2)(c) of Regulation 1182/71,

*"a period expressed in weeks, months or years shall start at the beginning of the first hour of the first day of the period, and shall end with the expiry of the last hour of whichever day in the last week, month or year is the same day of the week, or falls on the same date, as the day from which the period runs".*

The Court of Justice has confirmed that, for instance, if an event which is the point from which a period of a week starts to run happens on a Monday, the period will end on the following Monday, which will be the *dies ad quem* (deadline expiration date).<sup>37</sup> Likewise, if the time limit is expressed in months and the triggering event occurs on the 20th March, the period will end on the 20th April.

30. The start date ('*dies a quo*') in the application of Article 65(1)(a) GDPR consists of the day when the Chair and the competent supervisory authority have decided that the file is complete and the subject matter is referred to the EDPB by the Secretariat via the information and communication system mentioned in Article 17 of the EDPB Rules of Procedure.

---

<sup>32</sup> In cases where the withdrawal concerns the only objection which the LSA has decided not to follow or considered as not relevant and reasoned, the EDPB shall no longer be required to issue a binding decision in accordance with Article 65(1)(a) GDPR.

<sup>33</sup> Article 65(2) GDPR in conjunction with Article 11(4) RoP.

<sup>34</sup> Article 65(2) GDPR.

<sup>35</sup> Article 65(3) GDPR. See also paragraph 32.

<sup>36</sup> Regulation (EEC, Euratom) No 1182/71 of the Council of 3 June 1971 determining the rules applicable to periods, dates and time limits, O.J. 8.6.197, L 124/1. Article 40 RoP confirms that "*In order to calculate the periods and time limits expressed in the GDPR and in these Rules of Procedure, Regulation 1182/71 of the Council of 3 June 1971 determining the rules applicable to periods, dates and time limits shall apply*".

<sup>37</sup> See the Judgment in *Maatschap Toeters, MC Verberk v. Productschap Vee en Vlees*, C-171/03, ECLI:EU:C:2004:714, paragraph 33.

31. Since the GDPR does not express periods in working days, the time limits concerned include public holidays, Sundays and Saturdays<sup>38</sup>. However, when the last day of a period is a public holiday, Sunday or Saturday, the period shall end with the expiry of the last hour of the following working day<sup>39</sup>, thus the deadline expiration date ('*dies ad quem*') shall be the following working day.

### 3.3.2 Decision to extend by one month

32. Article 65(2) GDPR allows the first one-month deadline to be extended by a further month, taking into account the complexity of the subject-matter. The extension needs to be decided by the Chair of the EDPB, either on its own initiative or at the request of at least one third of the members of the EDPB<sup>40</sup>. The extension decision must be taken prior to the expiration of the one month deadline.

### 3.3.3 Extension by two weeks

33. The binding decision must in principle be adopted by two-thirds majority at the latest two months after the file has been considered complete and the subject-matter has been referred to the EDPB. However, if the EDPB has not been able to adopt a decision within the extended timeframe because the required majority is not reached, the EDPB shall then adopt the decision within two weeks following the expiration of the second month by simple majority of its members<sup>41</sup>.
34. During the two additional weeks, modifications can be made to the draft EDPB binding decision that was previously submitted for adoption by two-thirds majority if necessary to achieve the simple majority. In other words, the draft EDPB binding decision may be adapted and adjusted in case the two-thirds majority is not reached.

## 3.4 Preparation of the draft EDPB binding decision

35. According to Article 11(5) RoP, the binding decisions "*shall be prepared and drafted by the secretariat and, upon decision of the Chair, together with a rapporteur and expert subgroups members*"<sup>42</sup>. Therefore, the EDPB Secretariat should act as lead rapporteur and the Chair should decide on the involvement of an expert subgroup and of co-rapporteurs.
36. As soon as the LSA has submitted the matter to the EDPB for dispute resolution, the Secretariat should start the assessment of the completeness of the file. During this assessment, the Chair is invited to decide on the possible involvement of co-rapporteurs and will invite EDPB members to express an interest to become co-rapporteurs (unless the Chair decides not to involve co-rapporteurs for this case)<sup>43</sup>. In order to ensure fairness and impartiality, the (group of) co-rapporteur(s) should not include delegations from either the LSA or CSAs that submitted objections in relation to the draft decision<sup>44</sup>.

---

<sup>38</sup> Article 3(3) of Regulation 1182/71.

<sup>39</sup> Article 3(4) of Regulation 1182/71.

<sup>40</sup> Article 11(4) RoP.

<sup>41</sup> See Article 65(3) GDPR. Regarding the calculation of the majority and voting rights of EDPB members see further Section 3.5 (Adoption of the EDPB binding decision).

<sup>42</sup> See also Article 75(6)(g) GDPR, which provides that the Secretariat shall be responsible in particular for the preparation, drafting and publication of decisions on the settlement of disputes between supervisory authorities.

<sup>43</sup> If the call for expression of interests to serve as co-rapporteur is made prior to the assessment that the file is complete, care should be taken not to disclose any elements of the file until after the assessment has been made and the subject matter has been referred to the EDPB.

<sup>44</sup> See also the Judgment in *Dr. August Wolff GmbH & Co. KG Arzneimittel*, Case C-680/16 P, 27 March 2019, ECLI:EU:C:2019:257, paragraphs 29-41.

37. Finally, it should be noted that the Chair may also decide to involve the members of one or more other expert subgroups, depending on the needs of the case.
38. As indicated earlier, Article 11(2) RoP states that the EDPB shall take into account *only* the documents which were provided by the LSA and the other CSA(s) once the matter is referred to the EDPB. This means that the LSA or CSA(s) cannot during the drafting stage introduce new elements of fact supporting their respective positions.
39. In accordance with Article 76(1) GDPR, discussions of the Board and of expert subgroups shall be confidential when they concern the consistency mechanism<sup>45</sup>. Moreover, an obligation of professional secrecy is also imposed on the staff of all EEA national supervisory authorities<sup>46</sup>, the EDPS and the EDPB Secretariat<sup>47</sup>. This means that the duty of confidentiality and professional secrecy, which is of paramount importance, shall be respected by the EDPB and its members also in relation to Article 65(1)(a) dispute resolution cases. This concerns both the discussions and the documents exchanged.

### 3.5 Adoption of the EDPB binding decision

40. All majorities referred to by the GDPR (or by the RoP) refer to the total number of members of the EDPB entitled to vote, regardless of whether they are present or not<sup>48</sup>.
41. While not having the right to vote, EFTA EEA supervisory authorities (i.e. Iceland, Liechtenstein and Norway) shall have the right to express their positions on all items discussed and/or voted<sup>49</sup>.
42. In accordance with Article 68(6) GDPR, the EDPS shall have voting rights only on decisions which concern principles and rules applicable to the Union institutions, bodies, offices and agencies which correspond in substance to those of the GDPR. Where that is the case, the EDPS is entitled to vote on the decision as a whole.
43. Every EDPB member entitled to vote who is not represented at a plenary meeting can delegate its voting rights to another member of the Board entitled to vote and attending the plenary meeting<sup>50</sup>.
44. The majority required for the adoption of a binding decision under Article 65(1)(a) GDPR is two-thirds of the EDPB members entitled to vote<sup>51</sup>. Where the EDPB has been unable to adopt a decision by two-thirds majority, the EDPB shall adopt its decision within the following two weeks by simple majority. Where the members of the Board are split, the decision shall be adopted by the vote of the Chair<sup>52</sup>.

### 3.6 Notification to the supervisory authorities concerned

45. Once the EDPB has adopted its binding decision, the Chair of the EDPB shall notify the decision to all the supervisory authorities concerned without undue delay<sup>53</sup>. Therefore, all the CSAs in the case need to be notified of the binding decision.

<sup>45</sup> Article 33 RoP.

<sup>46</sup> Article 54 (2) GDPR.

<sup>47</sup> Article 56 of Regulation (EU) 2018/1725.

<sup>48</sup> Article 22(3) RoP.

<sup>49</sup> See the Decision of the EEA joint Committee No 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement [2018/1022], See also Recital (7) and Article 4(1) RoP.

<sup>50</sup> The Chair and the secretariat shall be notified of any delegation of voting rights. Article 22(5) RoP.

<sup>51</sup> Article 65(2) GDPR in conjunction with Article 22(3) RoP.

<sup>52</sup> Article 65(3) GDPR.

<sup>53</sup> Article 65(5) GDPR.

46. The notification will be performed by the Secretariat on behalf of the Chair via the information and communication system mentioned in Article 17 RoP<sup>54</sup>. The notification of the binding decision is performed via the notification of the decision in English, which is the only authentic language of the decision<sup>55</sup>. The supervisory authorities concerned will be deemed to be fully acquainted with the decision as notified<sup>56</sup>.

### 3.7 Final Decision of the supervisory authority(ies)

47. Within one month after the notification of the EDPB decision to the supervisory authorities, the LSA and/or CSA (as the case may be<sup>57</sup>) must adopt a final decision<sup>58</sup>. Each final decision must be adopted “on the basis of” the decision of the EDPB. Moreover, the final decision(s) must refer to the decision by the EDPB and must specify that this decision will be published on the EDPB website. The final decision(s) of the LSA and/or CSA shall also “attach” the decision of the EDPB<sup>59</sup>.

#### 3.7.1 “On the basis of”

48. The requirement of adopting a final decision “on the basis of” the EDPB decision reflects the fact that the EDPB’s decision is legally binding upon the LSA (and/or eventually the CSA(s) in case of need to adopt a final decision toward the data subjects<sup>60</sup>) as addressee(s) of the decision<sup>61</sup>.
49. The aim of the binding decision is to resolve conflicting views among the LSA(s) and CSA(s) on the merits of the case, in particular whether there is an infringement of the GDPR, in order to ensure the correct and consistent application of the GDPR in individual cases<sup>62</sup>.
50. The final decision must be adopted on the basis of the EDPB’s decision and must, therefore, give full effect to the binding direction(s) as set out in the EDPB’s decision. For example, if the EDPB has determined that there has indeed been an infringement of the GDPR, the LSA or CSA may not determine otherwise. In the same vein, if the EDPB has determined that envisaged action in relation to the controller or processor does not comply with the GDPR, the LSA or CSA must adapt their course of action accordingly<sup>63</sup>.

---

<sup>54</sup> Article 11.6 RoP.

<sup>55</sup> Article 11.6 RoP.

<sup>56</sup> Article 11.6 RoP. Urgent translations may be provided to authorities required to adopt a decision or take measures at national level on the basis of the EDPB binding decision in another EU language. Other supervisory authorities concerned can exceptionally request an urgent translation providing the reasons for such request. As the authentic language of the EDPB decision is English, the EDPB is not responsible for any use of the translations provided (Article 11.7 RoP).

<sup>57</sup> In case of partial or complete dismissal of a complaint, see Article 60(8) and (9) GDPR.

<sup>58</sup> Article 65(6) GDPR.

<sup>59</sup> The requirement that the final decision « attach » the EDPB decision does not mean that the EDPB decision must be annexed to the final decision within a single document (it is sufficient that the EDPB decision is communicated to the controller or processor together with the final decision).

<sup>60</sup> See Article 60(8) and (9) GDPR.

<sup>61</sup> Recital (136) and (143) GDPR.

<sup>62</sup> Recital (136) and Article 65(1)(a) GDPR.

<sup>63</sup> See Section 4 (Competence of the EDPB), in particular section 4.2 (Matters subject of the relevant and reasoned objection).

### 3.7.2 Decision(s) by LSA and/or CSA

51. The final decision of the LSA and, as the case may be, the CSA with whom the complaint has been lodged, shall be adopted under the terms of Article 60(7), (8) and (9) GDPR<sup>64</sup>.
52. The point of departure is that the LSA will be required to adopt and notify its final decision to the main establishment or single establishment of the controller or processor and inform the other supervisory authorities concerned as well as the EDPB of its final decision (including a summary of the relevant facts and grounds)<sup>65</sup>. One important derogation to this requirement concerns the situation where a complaint has been dismissed or rejected.
53. In cases where a complaint has been dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof<sup>66</sup>.
54. In case of need to take a decision to only partially dismiss a complaint, the LSA shall adopt the decision for the part concerning actions in relation to the controller or the processor, shall notify it to the main establishment or single establishment of the controller or processor on the territory of its Member State and shall inform the complainant thereof, while the supervisory authority of the complainant shall adopt the decision for the part concerning dismissal or rejection of that complaint, and shall notify it to that complainant and shall inform the controller or processor thereof<sup>67</sup>.
55. Each natural or legal person has the right to an effective judicial remedy before the competent national court against a decision of a supervisory authority which produces legal effects concerning that person, in line with Article 78 GDPR<sup>68</sup>.

### 3.7.3 Information to the EDPB

56. The LSA or, as the case may be, the CSA with which the complaint has been lodged, is required to inform the EDPB of the date when its final decision is notified respectively to the controller or the processor and to the data subject<sup>69</sup>.

## 3.8 Publication of the EDPB binding decision

57. In accordance with Article 65(5) GDPR, the publication of the EDPB binding decision on the website of the Board shall occur “without undue delay” after the LSA has notified the final national decision to the controller/processor and/or the CSA has notified the data subject (in case of a dismissal of a complaint). Whenever possible, “without undue delay” should be interpreted as suggesting that the publication of the EDPB binding decision should happen on the same day where the final national decision is notified to the controller/processor/complainant.
58. In order to allow the EDPB to publish its binding decision “without undue delay” after the notification of the final national decision, Article 65(6) GDPR requires the competent supervisory authority to inform the Board of the date when its final decision is notified respectively to the controller or processor and to the data subject. To avoid undue delays, each competent supervisory authority

---

<sup>64</sup> Article 65(6) GDPR.

<sup>65</sup> Article 60(7) GDPR.

<sup>66</sup> Article 60(8) GDPR.

<sup>67</sup> Article 60(9) GDPR.

<sup>68</sup> See also Recital (143) GDPR. See further Section 8 (Judicial remedies).

<sup>69</sup> Article 65(6) GDPR.

- should inform the Secretariat of the date on which notification of the national decision is expected to take place, preferably at least one day in advance.
59. Article 339 TFEU requires the members and staff of the EU institutions not to disclose information of the kind covered by the obligation of professional secrecy, in particular information about undertakings, their business relations or their cost components<sup>70</sup>. As a consequence, some portions of the EDPB binding decision may need to be redacted in order to avoid disclosure of information covered by professional secrecy. The Secretariat will evaluate the need to redact such elements on the basis of EU law and the case law of the CJEU<sup>71</sup>.

60. The EDPB will also publish the final national decision(s) in its register<sup>72</sup>, taking into consideration possible restrictions under national law of the competent supervisory authority concerning the publication of its decisions. Where such restrictions apply, the SAs should inform the Secretariat of any such restrictions.

## 4 COMPETENCE OF THE EDPB

61. The aim of the consistency mechanism, including Article 65(1)(a) GDPR, is to contribute to the **consistent application** of the GDPR throughout the Union. Recital (136) clearly indicates that the competence of the EDPB to issue a binding decision in case of conflicting views among LSA and CSAs in the context of the cooperation mechanism relates to the **merits of the case**, in particular whether there is an infringement of the GDPR<sup>73</sup>.
62. According to Article 65(1)(a) GDPR, the EDPB binding decision shall concern **all the matters which are the subject of the relevant and reasoned objection**. Therefore, the EDPB will assess **only** issues included in the objections that have been raised in relation to the draft or revised draft decision of the LSA. The EDPB will not reassess the whole case nor will it address issues that might be raised in the course of the Article 65 procedure but were not the subject of the reasoned and relevant objections submitted prior to the submission of the dispute to the EDPB.
63. The dispute between the LSA and the CSA(s) may concern either the fact that the LSA does not follow one or more relevant and reasoned objections or that the LSA is of the opinion that one or more

---

<sup>70</sup> An obligation of professional secrecy is also imposed on the staff of the EU institutions by the Staff Regulations and on the staff of the EDPS, including the EDPB Secretariat, also by Article 56 of Regulation (EU) 2018/1725. An obligation of professional secrecy is also imposed by Article 54 (2) GDPR on the members and staff of each supervisory authority.

<sup>71</sup> See, for instance, Judgments in *Bank Austria Creditanstalt*, T-198/03, 30 May 2006, ECLI:EU:T:2006:136; in *Evonik Degussa*, T-341/12, 28 January 2015, ECLI:EU:T:2015:51; in *Akzo Nobel NV*, T-345/12, 28 January 2015, ECLI:EU:T:2015:50; in *MasterCard, Inc.*, T-516/11, 9 September 2014, EU:T:2014:759; in *Stichting Greenpeace Nederland*, T-545/11 RENV, 21 November 2018, ECLI:EU:T:2018:817; in *Amicus Therapeutics UK Ltd*, T-33/17, 25 September 2018, ECLI:EU:T:2018:595; in *Pergan Hilfsstoffe für industrielle Prozesse GmbH*, Case T-474/04 , 12 October 2007, [2007] ECR II-4225.

<sup>72</sup> Article 70(1)(y) GDPR requires the EDPB to maintain a publicly accessible electronic register of decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism. See <https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions>.

<sup>73</sup> Recital (136) stipulates that "[...] The Board should also be empowered to adopt legally binding decisions where there are disputes between supervisory authorities. For that purpose, it should issue, in principle by a two-thirds majority of its members, legally binding decisions in clearly specified cases where there are conflicting views among supervisory authorities, in particular in the cooperation mechanism between the lead supervisory authority and supervisory authorities concerned on the merits of the case, in particular whether there is an infringement of this Regulation."

objections is not relevant or reasoned. The EDPB will assess, in relation to each objection raised, whether the objection meets the requirements of Article 4(24) GDPR and, if so, address the merits of the objection in the binding decision.

#### 4.1 Assessment of whether the objections are relevant and reasoned

64. In its Guidelines on relevant and reasoned objections, the EDPB has clarified the conditions that must be met in order for an objection to be considered “relevant and reasoned” within the meaning of Article 4(24) GDPR<sup>74</sup>.
65. When a LSA refers a dispute to the EDPB for resolution in accordance with Article 60(4) and 63 GDPR, the EDPB must first assess whether the objection(s) raised in fact meet the conditions of being relevant and reasoned<sup>75</sup>.
66. The EDPB recalls that in order for an objection to be considered as “relevant”, there must be a direct connection between the objection and the substance of the draft decision at issue. More specifically, the objection needs to concern either whether there is an infringement of the GDPR or whether the envisaged action in relation to the controller or processor complies with the GDPR<sup>76</sup>.
67. In order for an objection to be “reasoned”, it should be coherent, clear, precise and detailed in explaining the reasons for the objection. It should set forth, clearly and precisely, the essential elements on which the CSA based its assessment, and the link between the envisaged consequences of the draft decision (if it was to be issued as it is) and the significance of the anticipated risks for data subjects’ fundamental rights and freedoms and, where applicable, for the free flow of personal data within the Union<sup>77</sup>.
68. When assessing whether the objections in fact meet the conditions of being relevant and reasoned, the assessment carried out by the EDPB will be both **substantial and formal**. In other words, the EDPB will take into account the specific wording used by the CSA within each of the objections raised and whether each element of Article 4(24) GDPR is explicitly mentioned in relation to each specific objection; thus requiring an explicit reference to the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects<sup>78</sup>.
69. In its binding decision, the EDPB will not take any position on the merits of any substantial issues raised by objections that do not meet the conditions of Article 4(24) GDPR. If an objection does not meet the conditions of Article 4(24) GDPR, the binding decision of the EDPB remains without any prejudice to any assessments the EDPB may be called upon to make in other cases, including with the same parties, taking into account the contents of the relevant draft decision and the objections raised by the CSAs.

---

<sup>74</sup> RRO GLS, paragraphs 12-21.

<sup>75</sup> As clarified earlier, the LSA shall submit the matter to the EDPB either if it does not follow the relevant and reasoned objection *or* if it is of the opinion that the objection is not relevant or reasoned. See section 3.1 above.

<sup>76</sup> RRO GLS, paragraph 12. An objection raised fulfils the criterion of being “relevant” when, if followed, it would entail a change leading to a different conclusion as to whether there is an infringement of the GDPR or as to whether the envisaged action in relation to the controller or processor, as proposed by the LSA, complies with the GDPR. RRO GLS, paragraph 13.

<sup>77</sup> RRO GLS, paragraph 19. See also RRO GLS, paragraph 16. (“*In order for the objection to be “reasoned”, it needs to include clarifications and arguments as to why an amendment of the decision is proposed (i.e. the legal / factual mistakes of the LSA’s draft decision). It also needs to demonstrate how the change would lead to a different conclusion as to whether there is an infringement of the GDPR or whether the envisaged action in relation to the controller or processor complies with the GDPR.*”).

<sup>78</sup> See also RRO GLS, paragraphs 7 and 37.

## 4.2 Matters subject of the relevant and reasoned objection

70. In its Guidelines on relevant and reasoned objections, the EDPB also clarified the possible subject matter (substance) of a relevant and reasoned objection<sup>79</sup>. Those Guidelines describe a number of examples of objections that may meet the requirements of Article 4(24) GDPR. These examples relate to possible disagreements between the LSA and CSA on the following matters:

1. the existence of a given infringement of the GDPR;
2. the existence of additional or alternative infringements of the GDPR;
3. gaps in the draft decision justifying the need for further investigation;
4. insufficient factual information or reasoning;
5. procedural aspects; and
6. the specific action envisaged by the draft decision.

### 4.2.1 Existence of a given infringement of the GDPR

71. A first example of a possible relevant and reasoned objection involves the disagreement between the LSA and CSA as to whether or not a given provision of the GDPR has been infringed<sup>80</sup>. Such a disagreement may arise where the draft decision adopted by the LSA either:

- explicitly confirms the existence of an infringement of a specific article of the GDPR, but the CSA considers that this article of the GDPR has not been infringed<sup>81</sup>;
- explicitly confirms that a particular article of the GDPR has not been infringed, whereas the CSA considers that the article in question has been infringed.

72. In accordance with Article 65(1)(a) GDPR, the EDPB shall take a binding decision concerning all the matters which are the subject of the relevant and reasoned objections, “*in particular whether there is an infringement of the GDPR*”. The EDPB must make a binding decision which shall whenever possible, taking into account the elements of the file and the right to be heard, provide a final conclusion on the application of the GDPR in relation to the case at hand. In other words, the EDPB shall assess the merits of the arguments raised by the CSA in the objection against those of the LSA and make a final determination as to whether or not the given infringement of the GDPR took place or not. The EDPB will instruct the LSA to alter a finding of an infringement or to include one whenever necessary. In such cases, the LSA will then be obliged to implement the change in its final decision, taking into account the binding decision of the EDPB in relation to the objection raised.

### 4.2.2 Additional or alternative infringements of the GDPR

73. A second example of a possible relevant and reasoned objection involves disagreement between the LSA and CSA as to the conclusions to be drawn from the findings of the investigation. For instance, the objection may state that the findings amount to the infringement of a provision of the GDPR other than (and/or in addition to) those already analysed by the draft decision<sup>82</sup>.

74. As previously indicated, the EDPB must make a binding decision which shall whenever possible, taking into account the elements of the file and the respondent’s right to be heard, provide a final conclusion

---

<sup>79</sup> RRO GLS, paragraphs 22-48.

<sup>80</sup> RRO GLS, paragraphs 24-25.

<sup>81</sup> The RRO GLS include the following example : The CSA argues that LSA did not take into consideration the fact that the household exemption is not applicable to some of the processing operations conducted by a controller and involving the use of CCTV, hence that there is no infringement of the GDPR.

<sup>82</sup> RRO GLS, paragraph 26.

on the application of the GDPR in relation to the case at hand. This can potentially include a determination of the existence of additional (or alternative) infringements, provided that the file contains sufficient factual elements to substantiate the alleged infringement and the persons who would be adversely affected have been or can be heard in relation to the objections alleging the existence of an additional or alternative infringement<sup>83</sup>.

**Example 3:**

The draft decision of a LSA states that the controller failed to comply with the duty to inform pursuant to Article 14 GDPR (information to be provided where personal data have not been obtained from the data subject). The draft decision states that the controller should have provided the information in paragraphs 14(1) and 14(2)(a) and (e) GDPR and finds no other infringements of Article 14. One of the CSAs considers that the controller should have provided all the information referred to in Article 14(2)(b) and (f) GDPR, as the default position is that all such information set out in that subarticle should be provided to the data subject unless one or more categories of the information does not exist or is not applicable.<sup>84</sup> Provided the objection raised by the CSA meets the requirements of Article 4(24), and taking into account the elements of the file and the right to be heard, the EDPB will decide whether or not the controller additionally infringed Article 14(2)(b) and (f) GDPR, in addition to Article 14(1) and Art. 14(2)(a) and (e) GDPR.

75. If the EDPB determines, following a relevant and reasoned objection to this effect, that additional and/or alternative provisions of the GDPR have been infringed, the LSA will be obliged to reflect this in its final decision, taking into account the binding decision of the EDPB in relation to the objection raised.
76. It may be possible, in exceptional cases, that the file submitted to the EDPB does not contain sufficient factual elements to allow the EDPB to make a final conclusion regarding the existence of the infringement identified by the relevant and reasoned objection. In most cases, however, the information exchanged during the cooperation procedure should be sufficient to enable the CSA to substantiate its objection in such a way that the EDPB shall be able to make a final determination whether or not there has been an infringement of the GDPR<sup>85</sup>. Furthermore, when the LSA submits the matter to the Secretariat to obtain a binding decision on the basis of Article 65(1)(a) GDPR, the Secretariat may also request the LSA and/or CSA to provide additional information that is necessary to ensure the file is complete<sup>86</sup>.

#### 4.2.3 Gaps in the draft decision justifying the need for further investigation by the LSA

77. A third example of a possible relevant and reasoned objection involves disagreement between the LSA and CSA as to whether the draft decision has sufficiently investigated the relevant infringements of the GDPR<sup>87</sup>.

**Example 4:**

The LSA, upon receiving a complaint, considers that not all of the allegations of infringements contained in the complaint merit investigation. In its draft decision, the LSA only addresses those

<sup>83</sup> See section 5 regarding the right to be heard.

<sup>84</sup> See also Article 29 Working Party Guidelines on transparency under Regulation 2016/679, 29 November 2017, WP260 rev.01, 11 April 2018, paragraph 46.

<sup>85</sup> Where appropriate, the CSA and LSA can make use of Article 61 and 62 GDPR with a view of obtaining the necessary information prior to the issuance of the draft decision.

<sup>86</sup> See section 3.2 above.

<sup>87</sup> RRO GLS, paragraph 27.

aspects of the complaint which it decided to investigate without any statement regarding the other alleged infringements of the GDPR. The CSA considers that the LSA in its investigation unjustifiably failed to address a number of alleged infringements raised by the complainant and submits a relevant and reasoned objection based on the failure of the LSA to properly handle the complaint to safeguard the rights of the data subject.

78. Article 57(1)(f) GDPR imposes a duty upon supervisory authorities to handle each and every complaint submitted to them and to investigate the subject matter of the complaint “to the extent appropriate”. The term “to the extent appropriate” provides the competent supervisory authority with a margin of discretion as regards the extent or depth of the investigation needed. However, this discretionary power must be exercised with all due diligence<sup>88</sup> and in accordance with the relevant provisions of the GDPR implying mutual cooperation.
79. If the EDPB, on the basis of a relevant and reasoned objection, determines that the LSA has unjustifiably failed to investigate or in any other way address some of the issues raised by the complaint, the EDPB can issue a binding decision specifying the need for LSA to handle the matter further and to investigate – to the extent appropriate – the remaining subject matter of the complaint. To the extent that the draft decision allows it, the LSA should in principle first seek to finalise its draft decision as regards those matters that do not require further investigation within the deadline specified by Article 65(6).
80. For those matters requiring further investigation, it may be necessary for the LSA to open a new case file. In case a new case file is opened to address the remaining issues, the LSA is required to comply with all cooperation provisions under the GDPR. This may lead to submitting a new draft decision in accordance with A60(3) GDPR which addresses the outstanding alleged infringement. In situations where it is not possible for the LSA to follow this course of action (e.g., when there is inextricable link between the matter requiring further investigation and the other parts of the LSA’s draft decision that are to be finalised), it may be necessary for the LSA to first investigate the matter further and prepare an updated draft decision.
81. In any event, the LSA shall be required to further address the matter and keep the members of the EDPB informed of the steps taken. Moreover, the CSAs can seek to use the cooperation and consistency mechanisms provided for in the GDPR in case the LSA does not fulfil its obligations flowing from the Article 65 decision (i.e addressing the remaining issues to be resolved)<sup>89</sup>.

#### 4.2.4 Insufficient factual information or reasoning

82. A fourth example of a possible relevant and reasoned objection involves disagreement between the LSA and CSA as to whether sufficient factual elements and/or reasoning have been included in the draft decision<sup>90</sup>. For instance, a CSA might consider that the conclusion by the LSA included the draft

---

<sup>88</sup> Judgment in *Schrems*, C-362/14, 6 October 2015, ECLI:EU:C:2015:650, paragraph 63.

<sup>89</sup> The EDPB recalls the possibility for CSAs make use, where appropriate, of the ability to request mutual assistance pursuant to Article 61 GDPR (which also allow CSAs, in case the LSA fails to comply, to adopt a provisional measure in accordance with Article 66) or requests for an opinion pursuant to Article 64(2) GDPR (which is explicitly deemed by the legislator as particularly appropriate where a SA does not comply with its obligations for mutual assistance under Article 61 GDPR). The latter procedure may, eventually, produce a binding decision of the EDPB in accordance with Article 65(1)(c) GDPR. See also Advocate General Bobek, Opinion in *Facebook Ireland Limited*, C-645/19, ECLI:EU:C:2021:5, paragraphs 115-121. Additionally, the EDPB may also, in its binding decision under Article 65(1)(a) GDPR, invite the CSA to request the LSA to further investigate via an Article 61 Mutual Assistance request.

<sup>90</sup> RRO GLS, paragraph 29.

- decision is not adequately supported by the assessment carried out and the evidence presented<sup>91</sup>. In such a case the EDPB shall also be competent to issue a binding decision, provided the objection raised meets the whole threshold of Article 4(24) GDPR, including a link between the allegedly insufficient analysis and the existence of an infringement or the envisaged action<sup>92</sup>.
83. In a situation where the draft decision of the LSA contains insufficient factual elements or reasoning, there are essentially two possible scenarios.
  84. In the first scenario, the file on the basis of which the EDPB shall make its decision already contains sufficient information that would allow to address the lack of sufficient factual elements or reasoning in the draft decision. In such cases, the EDPB shall, within the scope of the relevant and reasoned objection, determine to what extent the LSA should amend its draft decision in order to remedy the insufficiency of reasoning, by making reference to the relevant elements included in the file.

**Example 5:**

The draft decision of the LSA establishes an infringement of the GDPR based on findings of fact supported by documentary evidence which were provided in the file to the EDPB. A number of CSAs submit relevant and reasoned objections outlining that the link between the documentary evidence and the finding of infringement is not sufficiently reasoned in the draft decision. The EDPB decision finds that the objection(s) are relevant and reasoned and indicates the correct legal interpretation and reasoning that the LSA should incorporate in its final decision.

85. In the second scenario, the file on the basis of which the EDPB shall make its decision does not contain sufficient factual elements to address the insufficiency of factual elements or reasoning.

**Example 6:**

The draft decision of the LSA finds that there is no infringement of Article 6(1)(a) GDPR and that the processing in question is lawful on the basis of the data subject's consent. However, neither the draft decision nor any other document in the file provides any further materials or analysis as to whether the conditions of Article 7 GDPR have been met. The draft decision simply states that the processing has been lawfully based on consent, without providing further reasoning or evidence. A CSA raises an objection against this lack of reasoning, arguing that the absence of this analysis gives rise to uncertainty surrounding the finding of no infringement in this case.

If the EDPB determines that the file on the basis of which the EDPB shall make its decision does not contain sufficient factual elements that would allow to remedy the insufficiency of reasoning, the EDPB can issue a binding decision specifying the need for LSA to investigate or address the matter further with a view of obtaining sufficient factual information, in line with what is specified in paragraphs 79-81 above.

#### 4.2.5 Procedural aspects

86. A fifth example of a possible relevant and reasoned objection involves a disagreement between the LSA and CSA as to whether the procedural requirements imposed by the GDPR have been properly respected and this affects the conclusion reached in the draft decision<sup>93</sup>.

---

<sup>91</sup> *Ibid.*

<sup>92</sup> RRO GLS, paragraph 29.

<sup>93</sup> RRO GLS, paragraph 30.

87. The EDPB recalls that the aim of the dispute resolution mechanism of Article 65(1)(a) GDPR is to resolve conflicting views on the merits of the case<sup>94</sup>. It is not intended to resolve possible disputes regarding procedural requirements or duties of cooperation<sup>95</sup>.
88. An objection involving a disagreement concerning procedural requirements will only be considered relevant and reasoned if the objection also puts forward arguments clarifying the different conclusion that the LSA should have reached in its draft decision. In its decision, the EDPB will resolve the dispute surrounding the conclusions reached in the draft decision.
89. If the procedural deficiencies leave the EDPB unable to resolve the dispute surrounding the conclusions reached by the draft decision (e.g. due to a lack of sufficient factual elements), the EDPB will recall the importance of the duty of cooperation and issue a binding decision specifying the need for LSA to investigate or address the matter further, in line with what is specified in paragraphs 79-81 above and ensuring full compliance with the procedural requirements in the GDPR which were not met.

#### 4.2.6 Action envisaged

90. A sixth example of a possible relevant and reasoned objection involves disagreement between the LSA and CSA as to whether the envisaged action in relation to the controller or processor complies with the GDPR<sup>96</sup>.
91. The EDPB recalls that Recital (150) GDPR states that the consistency mechanism may also be used to promote a consistent application of administrative fines. As a result, if the assessment of the EDPB within this context identifies shortcomings in the reasoning leading to the imposition of the fine at stake, the LSA will be instructed to re-assess the fine and remedy the identified shortcomings<sup>97</sup>.
92. Fines are by no means the only action a supervisory authority can envisage. A relevant and reasoned objection may therefore also relate to other envisaged actions, taking into account the range of powers listed in Article 58(2) GDPR. Each envisaged measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case<sup>98</sup>. In this context, it should be recalled that the decision to reject or dismiss a complaint, in whole or in part, also constitutes an envisaged action capable of being subject of a relevant and reasoned objection.

If the EDPB, on the basis of a relevant and reasoned objection, determines that the envisaged action included in the draft decision does not comply with the GDPR, it shall instruct the LSA to re-assess the envisaged action and change the draft decision in accordance with the binding decision of the EDPB.

## 5 THE RIGHT TO BE HEARD

### 5.1 Applicability

93. The right to be heard before an administration takes a measure that would adversely affect a person is enshrined in Article 41 CFEU and has long been recognised as a general principle of EU law<sup>99</sup>. The

---

<sup>94</sup> See above at paragraph 61.

<sup>95</sup> In this regard, the EDPB recalls Articles 61, 64(2), 65(1)(c) and 66 of the GDPR.

<sup>96</sup> See also RRO GLS, paragraphs 32 et seq.

<sup>97</sup> RRO GLS, paragraph 34.

<sup>98</sup> Recital (129) GDPR.

<sup>99</sup> See e.g. Judgment in *France v. Commission*, C-301/87, 14 February 1980, paragraph 29.

right to be heard is also included in Article 16 of the European Code of Good Administrative Behaviour and reflected in Article 11 RoP.

94. Article 41 CFEU is addressed not to the Member States but solely to the institutions, bodies, offices and agencies of the European Union<sup>100</sup>. Nevertheless, the right to be heard has also been recognised as "*inherent in respect for the rights of the defence, which is a general principle of EU law*"<sup>101</sup> and therefore also applies when Member States adopt decisions which come within the scope of EU law<sup>102</sup>.
95. The right to be heard applies to administrative proceedings of which the outcome is likely to affect the (legal or natural) person's interests. It also applies in situations where the administration of EU law is divided or shared between EU and the Member States (so-called "composite procedures"<sup>103</sup>). Article 41(2)(a) CFEU is framed in terms of individual measures that would adversely affect the person, with no specific requirement that the contested measure should be initiated against that person<sup>104</sup>.
96. Article 65(2) GDPR provides that the EDPB's decision "*shall be [...] addressed to the lead supervisory authority and all the supervisory authorities concerned and binding on them*". Article 65(2) GDPR reflects the fact that the binding decision of the EDPB aims to resolve a dispute that has emerged among two or more national supervisory authorities. In accordance with the procedure under Article 60 GDPR, LSA will have shared its legal analysis in the draft decision and in relation the objections raised during the cooperation procedure. The CSA(s) likewise will have shared its (their) objection(s) in relation to the draft decision, including any materials to substantiate their objection. In addition, both the LSA and CSAs can share their views in the course of the preparation and adoption of the EDPB decision<sup>105</sup>.
97. Article 65(2) GDPR also confirms that the EDPB decision does not address directly any party other than the LSA and CSAs. Nevertheless, the decision adopted by the EDPB at European level shall be binding on the LSA or, as the case may be, the CSA with which the complaint has been lodged and is therefore decisive for the outcome of the procedure at national level. It therefore also may affect the interests of persons who were part of the procedure that gave rise to the draft decision.
98. As a result, any of these persons which would be adversely affected by the decision, in particular the controller(s) and/or processor(s) who are addressed by the draft decision of the LSA, as well as any other person which would be adversely affected by the decision, must be afforded the right to be

---

<sup>100</sup> See e.g. Judgment in *Cicala*, C-482/10, 21 December 2011, ECLI:EU:C:2011:868, paragraph 28.

<sup>101</sup> See e.g. Judgment in *Mukarubega*, C-166/13, 5 November 2014, ECLI:EU:C:2014:2336, paragraph 45.

<sup>102</sup> *Ibid.*, paragraph 46. See also Judgments in *Glencore Agriculture Hungary Kft.*, C-189/18, 16 October 2019, ECLI:EU:C:2019:861, paragraph 39 ("[...] *The authorities of the Member States are subject to that obligation when they take decisions which come within the scope of EU law, even though the EU law applicable does not expressly provide for such a procedural requirement*") and in *Teodor Ispas*, Case C-298/16, 9 November 2017, ECLI:EU:C:2017:843, paragraph 26. See also the Opinion of Advocate General Bobek in *Teodor Ispas*, Case C-298/16, 7 September 2017, ECLI:EU:C:2017:650, paragraphs 35-69.

<sup>103</sup> Regarding composite administrative procedures, see e.g. the Opinion of Advocate General Compos Sánchez-Bordana in *Silvio Berlusconi*, Case C-219/17, 27 June 2018, ECLI:EU:C:2018:502, paragraphs 57-79. See also F. Brito Bastos, "Beyond Executive Federalism. The Judicial Crafting of the Law of Composite Administrative Decision-Making", Thesis submitted for assessment with a view to obtaining the degree of Doctor of Laws of the European University Institute, Florence, 13 June 2018, in particular at p. 120-163.

<sup>104</sup> P. Craig, "Article 41 - Right to Good Administration", in *EU Charter of Fundamental Rights : A Commentary*, edited by Steve Peers, et al., Bloomsbury Publishing, 2014, p. 1079.

<sup>105</sup> However, according to the RoP, in exceptional circumstances, the EDPB can decide to consider further documents (Article 11(2) in fine RoP).

heard in relation to the subject matter which is brought before the EDPB pursuant to Articles 60(4), 63 and 65(1)(a) GDPR.

## 5.2 Purpose

99. The right to be heard is described by the Court as guaranteeing “*every person the opportunity to make known his views effectively during an administrative procedure and before the adoption of any decision liable to affect his interests adversely*”<sup>106</sup>. As clarified by the CJEU, the purpose of the rule, that the addressee of an adverse decision must be placed in a position to submit his observations before that decision is taken, is to put the competent authority in a position effectively to take all relevant information into account. In order to ensure that the person concerned is in fact protected, the purpose of that rule is, *inter alia*, to enable that person to correct an error or submit such information relating to his or her personal circumstances as will argue in favour of the adoption or non-adoption of the decision, or in favour of it having a specific content<sup>107</sup>.
100. The right to respond is also part of the right to be heard since an “*administrative procedure requires that the person concerned should be able [...] to put his own case and properly make his views known on the relevant circumstances and, where necessary, on the documents taken into account by the Community institutions*”<sup>108</sup>. Except in cases where legislation expressly provides for the possibility of an oral hearing, such as in the competition proceedings, the right to be heard does not necessarily require an oral hearing<sup>109</sup>.

## 5.3 Timing

### 5.3.1 At national level and prior to referral to the EDPB

101. Before the EDPB is given the task of issuing a binding decision, every supervisory authority is under and obligation to respect the right to be heard in the context of its national procedure, as a general principle of EU law<sup>110</sup>. Indeed, every supervisory authority needs to “*respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken*”<sup>111</sup>. The right to be heard applies regardless of whether the case is cross-border in nature or not.
102. Even in the absence of specific provisions under national law, the LSA should, in advance of triggering Article 65(1)(a) GDPR, ensure that procedure conducted at national level takes into account the requirements of the right to be heard as a general principle of EU law.

### 5.3.2 During the assessment of completeness of the file

103. When the LSA submits the matter to the Secretariat with a view of obtaining a binding decision of the EDPB under Article 65(1)(a) GDPR, the Secretariat should assess which persons would possibly be adversely affected by the EDPB decision in the sense of Article 41 of the Charter. It should also assess whether each of those persons was offered the opportunity to exercise its right to be heard.

---

<sup>106</sup> See e.g. Judgments in *M.M.*, C-277/11, 22 November 2012, EU:C:2012:744, paragraph 87; *Mukarubega*, paragraph 46; *Glencore Agriculture Hungary*, paragraph 39 and the case law cited therein.

<sup>107</sup> Judgment in *Glencore*, paragraph 41 and 52.

<sup>108</sup> See e.g. the Judgment in *Technische Universität Munchen*, C-269/90, 21 November 1991, paragraph 25.

<sup>109</sup> See Article 12 of Regulation 773/2004 (O.J. 27 April 2004, L 123, p. 18). See also the Opinion of Advocate General Wahl in *SKW Stahl-Metallurgie GmbH and Holding AG v European Commission*, C-154/14, 3 September 2015, ECLI:EU:C:2015:543, paragraphs 45-47.

<sup>110</sup> See paragraph 94 above.

<sup>111</sup> Recital (129) GDPR.

104. It is not sufficient that the LSA has heard the persons who might be adversely affected in the course of the national procedure prior to the adoption of its draft decision within the meaning of Article 60(3) GDPR. Before the EDPB will be in a position to resolve the dispute, the right to be heard must also be afforded in relation to any objections raised in relation to the draft decision, in particular where the LSA chooses not to follow the objection (or considers it as not being relevant and/or reasoned).

105. When submitting the matter to the Secretariat, the LSA is expected to demonstrate how the right to be heard has been afforded to persons benefitting from this right in the course of the national procedure leading to the draft decision. As regards the documents shared when submitting the matter to the Secretariat, the LSA should specifically mention whether or not these documents (or the relevant contents thereof<sup>112</sup>) were subject to the right to be heard and with regard to which persons<sup>113</sup>. Replies or summaries of the hearing(s) should be provided as well.

106. The accommodation of the right to be heard is an essential element of the procedure, in the absence of which the subject matter of the dispute cannot be settled by the EDPB. As a result, the gathering and verification of the relevant information is carried out in the context of the check on the completeness of the file, before the subject matter is referred to the EDPB. Only after all the relevant verifications have been made by the Secretariat, the Chair shall be in the position to declare the file complete<sup>114</sup>.

107. If there are relevant documents or information that have not been subject to the right to be heard, the Chair may instruct the Secretariat to ask the supervisory authorities (LSA / CSA) to take the necessary actions to enable any party that could be affected to be heard. If necessary, the Chair may instruct the Secretariat to take measures to directly ensure the right to be heard at the EDPB level. In both instances, the persons who would be adversely affected shall be invited to exercise the right to be heard on the relevant documents or information within a specific timeframe, taking into account the complexity of the subject matter (as well as possible needs for translation).

## 6 ACCESS TO THE FILE

108. The right to good administration includes the right of every person to have access to the file, while respecting the legitimate interests of confidentiality and of professional and business secrecy<sup>115</sup>.

109. Access to the documents and information that form the basis of an administrative decision is closely connected with the right to be heard<sup>116</sup>. In accordance with that principle, ‘the addressees of decisions

---

<sup>112</sup> For purposes of the procedure under Article 65(1)(a) GDPR, the scope of which is limited resolving disputes concerning the objections raised, the right to be heard does not need to extend to elements beyond the subject matter of the dispute.

<sup>113</sup> See Article 11(2)(f) RoP, which specifies that the LSA when submitting the matter to the Secretariat should include, *inter alia*, ““in accordance with Article 41 of the European Charter on Fundamental Rights, the written observations the LSA collected from the persons that might be adversely affected by the Board’s decision, together with confirmation and evidence of which documents submitted to the Board were provided to them when they were invited to exercise their right to be heard or a clear identification of the elements for which it is not the case”.

<sup>114</sup> See also section 3.2 above.

<sup>115</sup> Article 41(2)b CFEU. The SA acting on behalf of the EDPB cannot make a general reference to confidentiality to justify a total refusal to disclose documents in its file to persons adversely affected, nor can it give blank pages on the ground that they contained business secrets without providing a more comprehensible non-confidential version, or a summary of the documents.

<sup>116</sup> Opinion of Advocate General Bobek in *Teodor Ispas*, Case C-298/16, 7 September 2017, ECLI:EU:C:2017:650, paragraphs 117 and following.

which significantly affect their interests must be placed in a position in which they can effectively make known their views as regards the *information on which the authorities intend to base their decision*<sup>117</sup>.

110. The right of access to the file of the EDPB as part of the right to good administration is distinct from the general right of access to documents held by the European institutions, bodies, offices and agencies pursuant to Regulation (EC) No 1049/2001<sup>118</sup>, Article 15(3) TFEU or Article 42 of the Charter<sup>119</sup>. The right of access to the file and the right of access to documents are subject to different criteria and exceptions and pursue different purposes.
111. The right of access to the file extends to the documents shared with the EDPB to resolve the dispute in accordance with Article 65(1)(a) procedure, save where they involve business secrets of other undertakings, confidential information, as assessed by the EDPB on a case by case basis.
112. The right of access to the file shall not extend to confidential information and internal documents of the EDPB or the SAs (e.g. email correspondence or preparatory documents). In particular, the right of access shall not extend to exchanges between the EDPB and its members once the procedure has been launched<sup>120</sup>.

---

<sup>117</sup> Opinion of Advocate General Bobek in *Teodor Ispas*, Case C-298/16, 7 September 2017, ECLI:EU:C:2017:650, paragraphs 117 and following. See in the same vein also Opinion of Advocate General Bobek in *Glencore Agriculture Hungary Kft.*, C-189/18, 16 October 2019, ECLI:EU:C:2019:861, paragraph 51

<sup>118</sup> Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43). Article 2(1) of Regulation (EC) No 1049/2001 sets out that any citizen of the EU, and any natural or legal person residing or having its registered office in a Member State, has a right of access to documents of the EU institutions, subject to the principles, conditions and limits defined in that Regulation.

<sup>119</sup> Article 32 RoP.

<sup>120</sup> See also Article 33 RoP.

## 7 THE DUTY TO GIVE REASONS

113. The right to good administration contained in Article 41 CFEU also includes the obligation of the administration to give reasons for its decisions<sup>121</sup>.
114. The duty to give reasons entails informing the addressee of the decision of the **factual and legal grounds** on which it is based, thereby enabling the person to decide whether to seek judicial review and facilitate the exercise of that review by the courts<sup>122</sup>.
115. The EDPB must articulate, in a clear and unequivocal fashion the reasoning underlying in its decision in such a way as to enable the persons affected to ascertain the reasons for its decision. While the EDPB does not need to state *all* legal and factual reasons leading to its decision, it must explain those which were of *decisive importance*<sup>123</sup>. In the same vein, the EDPB is also not obliged to adopt an explicit position on all the arguments raised. It is sufficient for the decision to set out, in a clear and unambiguous manner, the principal issues of law and of fact upon which it is based and which are necessary in order that the reasoning which has led the EDPB to its decision may be understood. What ultimately matters is that the statement of reasons by the EDPB enables all persons affected by the decision to ascertain whether the relevant provisions have been applied correctly.
116. The EDPB must in its statement of reasons set out all the relevant grounds and motives for the adoption of its decision – including those that originate from the national level. This means that insofar as the facts set out in the draft decision or related documents are decisive for the decision of the EDPB, then the EDPB should include them in its statement of reasons<sup>124</sup>.
117. In relation to objections where the EDPB simply agrees with the reasons contained in the draft decision by the LSA or the decision of the LSA not to follow the relevant and reasoned objection (or to consider them not relevant or reasoned), the EDPB may fulfil its duty to state reasons by simply referring back to the position of the LSA, provided the affected persons were informed of those positions of the LSA and given the opportunity to be heard in relating to those positions<sup>125</sup>.
118. In light of the aforementioned considerations, the binding decision adopted by the EDPB on the basis of Article 65(1)(a) GDPR should in principle include a summary of dispute as well as an assessment of whether the conditions for adopting a binding decision are met. For each objection raised, the EDPB will then in principle<sup>126</sup>:
- summarise main elements of the draft decision which are related to the subject matter of the objection;

---

<sup>121</sup> Article 41(2)c CFEU.

<sup>122</sup> See e.g., Judgment in *Métropole Télévision SA*, T-206/99, 21 March 2011, paragraph 44. See also P. Craig, "Article 41 - Right to Good Administration", in *EU Charter of Fundamental Rights: A Commentary*, edited by Steve Peers, et al., Bloomsbury Publishing, 2014, p. 1085.

<sup>123</sup> See e.g. Judgments of the General Court in *L'Air liquide*, Cases T-185/06, 16 June 2011, EU:T:2011:275, paragraph 64; in *Ryanair Ltd*, T-123/09, 28 March 2012, EU:T:2012:164, paragraph 178-179; and in *FIH Holding A/S*, T-386/14, 15 September 2016, EU:T:2016:474, paragraph 94.

<sup>124</sup> Based on F. Brito Bastos, "Beyond Executive Federalism. The Judicial Crafting of the Law of Composite Administrative Decision-Making", Thesis submitted for assessment with a view to obtaining the degree of Doctor of Laws of the European University Institute, Florence, 13 June 2018, p. 176 and following.

<sup>125</sup> *Ibid.*

<sup>126</sup> The draft binding decision of the EDPB should in principle synthesize the main elements of facts preceding the dispute, together with a summary of the main arguments put forth, unless the specific wording used is essential for a proper discussion/understanding of the issue at stake.

- summarise the main elements of the objection raised;
- summarise the position of the LSA or CSA in relation to the objection raised; and
- summarise the position of the persons who may be adversely affected in relation to the objection.

Once the relevant elements have been set out, the EDPB will assess, in relation to each objection raised, whether the EDPB meets requirements of Article (24) GDPR and, if so, address the merits of the objection in the binding decision<sup>127</sup>.

119. The operative parts of the decision should be clearly identified as such and included at the end of the decision, rendering explicit to what extent the competent authority is required/not required to amend its draft decision before finalisation.

## 8 JUDICIAL REMEDIES

120. Article 47 of the Charter guarantees the right to an effective remedy and to a fair trial. This is linked to the need to ensure the compatibility of the acts of the EU institutions with the European Union legal order, which is a task generally entrusted to the Court of Justice and to the courts of the European Union.

121. Good administrative behaviour entails informing persons affected by the measure of the available appeal mechanism<sup>128</sup>. The EDPB decision will refer to the possibilities open to appeal it (i.e. to seek annulment), whereas the competent supervisory authority will refer to the appeal mechanisms available at national level. The competent supervisory authority may in its final decision also choose make reference to the possibilities to seek annulment of the decision of the EDPB on the basis of which the final decision was adopted, as clarified by Recital (143) GDPR (in addition to providing information regarding possible appeal mechanisms at national level in relation to its final decision).

122. While Recital (143) refers to the possibility of persons directly and individually concerned by a decision of the EDPB bringing an action for annulment before the CJEU, the position on standing will ultimately be assessed by the CJEU in light of the conditions provided for in Article 263 TFEU<sup>129</sup>.

---

<sup>127</sup> It should be noted that the EDPB does not take any position on the merit of any substantial issues raised by objections deemed not to meet the requirements stipulated by Article 4(24) GDPR. Where that is the case, the decision of the EDPB is without any prejudice to any assessments the EDPB may be called upon to make in other cases, including with the same parties, taking into account the contents of the relevant draft decision and the objections raised by the CSAs.

<sup>128</sup> See also Commission ‘Code of Good administrative behaviour’, Point 3, third indent: ‘Where Community law so provides, measures notified to an interested party should clearly state that an appeal is possible and describe how to submit it, (the name and office address of the person or department with whom the appeal must be lodged and the deadline for lodging it). Where appropriate, decisions should refer to the possibility of starting judicial proceedings and/or of lodging a complaint with the European Ombudsman in accordance with Article 230 or 195 of the Treaty establishing the European Community.’ European Ombudsman ‘Code of Good administrative behaviour’, Article 19 - indication of the possibilities of appeal: ‘A decision of the Institution which may adversely affect the rights or interests of a private person shall contain an indication of the appeal possibilities available for challenging the decision. It shall in particular indicate the nature of the remedies, the bodies before which they can be exercised, as well as the time limits for exercising them. Decisions shall in particular refer to the possibility of judicial proceedings and complaints to the European Ombudsman under the conditions specified in, respectively, Articles [263] and Articles [228 TFEU].’

<sup>129</sup> See Order of the General Court of 7 December 2022, WhatsApp Ireland Ltd, T-709/21, ECLI:EU:T:2022:783 in particular at paragraphs 33 and following.

123. An action for annulment before the Court of Justice does not suspend the effects of the decision of the EDPB<sup>130</sup>. The competent SAs will therefore still have to comply with the decision of the EDPB adopted on the basis of Article 65(1)(a) GDPR, notwithstanding the appeal. This is without prejudice to the right to effective judicial remedy by the controller or processor at national level in accordance with Article 78 GDPR.

## 8.1 Supervisory authorities

124. Article 65(2) GDPR makes clear that decisions adopted by the EDPB on the basis of Article 65(1)(a) GDPR are binding upon the lead supervisory authority and all the concerned supervisory authorities. National SAs must adopt their final decision on the basis of the EDPB decision. Article 65(2) also makes clear the decision is an act “addressed to” the LSA and the CSAs - it does not directly address any third parties<sup>131</sup>.

125. According to Recital (143) GDPR, as addressees of the decisions of the Board, the concerned supervisory authorities which wish to challenge them have to bring action within two months of being notified of them, in accordance with Article 263 TFEU. This means, *inter alia*, that the supervisory authorities acting before the Court of Justice against a binding decision of the EDPB would need to do so relying on one of the listed grounds for annulment contained in Article 263 TFEU.

126. Although only the LSA and some CSAs (pursuant to Article 60(8) and (9) GDPR) shall adopt their national decision on the basis of the EDPB binding decision, the decision is addressed to all the CSAs involved in the cross-border case. Article 65(2) GDPR mentions all the CSAs as addressees of the decision and the final national decision is the product of a co-decision making process which is strongly affected by the decision of the EDPB. As a consequence, all the supervisory authorities that are concerned in a given cross-border case (see Article 4(22) GDPR) are “addressed” by the decision and therefore entitled to bring action for annulment of the EDPB decision.

127. Although the supervisory authorities concerned, as Members of the EDPB, gain knowledge of the content of the EDPB binding decision in the occasion of its adoption pursuant to Article 65(2) GDPR, the time limitation for them to bring action will start when the decision is notified to them by the EDPB Secretariat, acting on behalf of the Chair<sup>132</sup> and using the internal information and communication system<sup>133</sup>.

---

<sup>130</sup> Article 278 TFEU (ex Article 242 TEC): “Actions brought before the Court of Justice of the European Union shall not have suspensive effect. The Court may, however, if it considers that circumstances so require, order that application of the contested act be suspended.”

<sup>131</sup> See also paragraph 97 above.

<sup>132</sup> See, e.g. Judgment of the General Court in *Access Info Europe v Council*, T-233/09, ECLI:EU:T:2011:105, paragraph 28 (“Where the addressee has been notified, it is the date of notification which is to be taken into consideration for the purposes of calculating the time allowed [...] for bringing proceedings, not the date on which cognisance was taken, which comes into play only as an alternative in cases where there is no notification”).

<sup>133</sup> See Article 17 EDPB RoP.

## 8.2 Controller, processor, complainant, or other entity

128. Entities other than the addressees may be entitled to act before the Court of Justice for the annulment of the EDPB binding decision if the decision is of direct and individual concern to them, under the conditions set in Article 263 TFEU<sup>134</sup>.
129. Recital (143) explicitly mentions that controllers, processors, or complainants may be directly and individually concerned by an EDPB binding decision. These requirements are, however, interpreted restrictively by the Court of Justice and therefore a case-by-case analysis is necessary<sup>135</sup>.
130. Without prejudice to the right under Article 263 TFEU, each natural or legal person also has an effective judicial remedy before the competent national court against those final decisions taken by supervisory authorities, which produces legal effects concerning that person<sup>136</sup>. This right has to be exercised in accordance to the applicable national legislation. Article 78(4) GDPR specifies that where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or decision of the Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.
131. Where a decision of a supervisory authority implementing an Article 65 GDPR decision of the EDPB is challenged before a national court and the validity of the decision of the EDPB is at issue, the national court does not have the power to declare the EDPB's Article 65 GDPR decision invalid. Where it considers the decision invalid, it must refer the question of validity to the Court of Justice in accordance with Article 267 TFEU<sup>137</sup>.
132. However, a national court may not refer a question on the validity of a decision of the EDPB when the requesting natural or legal person was under the legal conditions to bring an action for annulment of that decision before the CJEU (in particular if it was directly and individually concerned), but had not done so within the two-month period laid down in Article 263 TFEU. Therefore, when the directly and individually concerned persons decide to not bring an action for annulment of the EDPB binding decision, this will prevent them from challenging the validity of the EDPB binding decision in front of national courts.

---

<sup>134</sup> Recital (143) GDPR.

<sup>135</sup> See also the Opinion of Advocate General Bobek in *Facebook Ireland Limited*, C-645/19, ECLI:EU:C:2021:5, footnote 52 and Order of the General Court of 7 December 2022, WhatsApp Ireland Ltd, T-709/21, ECLI:EU:T:2022:783 in particular at paragraphs 33 and following.

<sup>136</sup> Recital (143) GDPR. This includes the exercise of investigative, corrective, and authorisation powers, or the dismissal or rejection of complaints, but not including non-legally binding measures.

<sup>137</sup> Recital (143) GDPR.

# Guidelines



**Guidelines 01/2022 on data subject rights - Right of access**

**Version 2.1**

**Adopted on 28 March 2023**

## Version history

Version 1.0	18 January 2022	Adoption of the Guidelines for public consultation
Version 2.0	28 March 2023	Adoption of the Guidelines after public consultation
Version 2.1	30 May 2024	Minor corrections

## EXECUTIVE SUMMARY

The right of access of data subjects is enshrined in Art. 8 of the EU Charter of Fundamental Rights. It has been a part of the European data protection legal framework since its beginning and is now further developed by more specified and precise rules in Art. 15 GDPR.

### Aim and overall structure of the right of access

The overall aim of the right of access is to provide individuals with sufficient, transparent and easily accessible information about the processing of their personal data so that they can be aware of and verify the lawfulness of the processing and the accuracy of the processed data. This will make it easier - but is not a condition - for the individual to exercise other rights such as the right to erasure or rectification.

The right of access according to data protection law is to be distinguished from similar rights with other objectives, for example the right of access to public documents which aims at guaranteeing transparency in public authorities' decision-making and good administrative practice.

However, the data subject does not have to give reasons for the access request and it is not up to the controller to analyse whether the request will actually help the data subject to verify the lawfulness of the relevant processing or exercise other rights. The controller will have to deal with the request unless it is clear that the request is made under other rules than data protection rules.

The right of access includes three different components:

- Confirmation as to whether data about the person is processed or not,
- Access to this personal data and
- 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.

### General considerations on the assessment of the data subject's request

When analysing the content of the request, the controller must assess whether the request concerns personal data of the individual making the request, whether the request falls within the scope of Art. 15 and whether there are other, more specific, provisions that regulate access in a certain sector. It must also assess whether the request refers to all or only parts of the data processed about the data subject.

There are no specific requirements on the format of a request. The controller should provide appropriate and user-friendly communication channels that can easily be used by the data subject. However, the data subject is not required to use these specific channels and may instead send the request to an official contact point of the controller. The controller is not obliged to act on requests that are sent to completely random, or apparently incorrect, addresses.

Where the controller is not able to identify data that refers to the data subject, it shall inform the data subject about this and may refuse to give access unless the data subject provides additional information that enables identification. Further more, if the controller has doubts about whether the data subject is who they claim to be, the controller may request additional information in order to confirm the identity of the data subject. The request for additional information must be proportionate

to the type of data processed, the damage that could occur etc. in order to avoid excessive data collection.

### **Scope of the right of access**

The scope of the right of access is determined by the scope of the concept of personal data as defined in Art. 4(1) GDPR. Aside from basic personal data like name, address, phone number etc. a broad variety of data may fall within this definition like medical findings, history of purchases, creditworthiness indicators, activity logs, search activities etc. Personal data which have undergone pseudonymisation are still personal data as opposed to anonymised data. The right of access refers to personal data concerning the person making the request. This should not be interpreted overly restrictively and may include data that could concern other persons too, for example communication history involving incoming and outgoing messages.

In addition to providing access to the personal data, the controller has to provide additional information about the processing and on data subjects' rights. Such information can be based on what is already compiled in the controller's record of processing activities (Art. 30 GDPR) and the privacy notice (Art. 13 and 14 GDPR). However, this general information may have to be updated to the time of the request or tailored to reflect the processing operations that are carried out in relation to the specific person making the request.

### **How to provide access**

The ways to provide access may vary depending on the amount of data and the complexity of the processing that is carried out. Unless explicitly stated otherwise, the request should be understood as referring to *all* personal data concerning the data subject and the controller may ask the data subject to specify the request if they process a large quantity of data.

The controller will have to search for personal data throughout all IT systems and non-IT filing systems based on search criteria that mirrors the way in which the information is structured, for example name and customer number. The communication of data and other information about the processing must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The more precise requirements in this regard depend on the circumstances of the data processing as well as the data subject's ability to grasp and comprehend the communication (for example taking into account that the data subject is a child or a person with special needs). If the data consists of codes or other "raw data", these may have to be explained in order to make sense to the data subject.

The main modality for providing access is to provide the data subject with a copy of their data but other modalities (such as oral information and on site access) can be foreseen if the data subject requests it. The data can be sent by e-mail, provided that all necessary safeguards are applied taken into consideration, for example, the nature of the data, or in other ways, for example a self-service tool.

Sometimes, when there is a large quantity of data and it would be difficult for the data subject to comprehend the information if given all in one bulk – especially in the online context - the most appropriate measure could be a layered approach. Providing information in different layers may facilitate the data subject's understanding of the data. The controller must be able to demonstrate that the layered approach has an added value for the data subject and all layers should be provided at the same time if the data subject chooses it.

The copy of the data and the additional information should be provided in a permanent form such as written text, which could be in a commonly used electronic form, so that the data subject can easily download it. The data can be given in a transcript or a compiled form as long as all the information is included and this does not alter or change the content of the information.

The request must be fulfilled as soon as possible and in any event within one month of receipt of the request. This can be extended by two further months where necessary, taking into account the complexity and number of the request. The data subject then has to be informed about the reason for the delay. The controller must implement necessary measures to deal with requests as soon as possible and adapt these measures to the circumstances of the processing. Where data is stored only for a very short period, there must be measures to guarantee that a request for access can be fulfilled without the data being erased while the request is being dealt with. Where a large quantity of data is processed, the controller will have to put in place routines and mechanisms that are adapted to the complexity of the processing.

The assessment of the request should reflect the situation at the moment when the request was received by the controller. Even data that may be incorrect or unlawfully processed will have to be provided. Data that has already been deleted, for example in accordance with a retention policy, and therefore is no longer available to the controller cannot be provided.

### **Limits and restrictions**

The GDPR allows for certain limitations of the right of access. There are no further exemptions or derogations. The right of access is without any general reservation to proportionality with regard to the efforts the controller has to take to comply with the data subject's request.

According to Art. 15(4) the right to obtain a copy shall not adversely affect the rights and freedoms of others. The EDPB is of the opinion that these rights must be taken into consideration not only when granting access by providing a copy, but also, if access to data is provided by other means (on-site access for example). Art. 15(4) is not, however, applicable to the additional information on the processing as stated in Art. 15(1) lit. a.-h. The controller must be able to demonstrate that the rights or freedoms of others would be adversely affected in the concrete situation. Applying Art. 15(4) should not result in refusing the data subject's request altogether; it would only result in leaving out or rendering illegible those parts that may have negative effects for the rights and freedoms of others.

Art. 12(5) GDPR allows controllers to reject requests that are manifestly unfounded or excessive, or to charge a reasonable fee for such requests. These concepts have to be interpreted narrowly. Since there are very few prerequisites regarding access requests, the scope of considering a request as manifestly unfounded is rather limited. Excessive requests depend on the specifics of the sector in which the controller operates. The more often changes occur in the controller's data base, the more often the data subject may be permitted to request access without it being excessive. Instead of refusing access, the controller may decide to charge a fee from the data subject. This would only be relevant in the case of excessive requests in order to cover the administrative costs that such requests may cause. The controller must be able to demonstrate the manifestly unfounded or excessive character of a request.

Restrictions of the right of access may also exist in Member States' national law as per Art. 23 GDPR and the derogations therein. Controllers who intend to rely on such restrictions must carefully check the requirements of the national provisions and take note of any specific conditions that may apply. Such conditions may be that the right of access is only temporarily delayed or that the restriction only applies to certain categories of data.

## Table of contents

1	Introduction - general observations.....	8
2	Aim of the right of access, structure of Article 15 GDPR and general principles.....	10
2.1	Aim of the right of access .....	10
2.2	Structure of Article 15 GDPR .....	11
2.2.1	Defining the content of the right of access .....	12
2.2.1.1	Confirmation as to ‘whether’ or not personal data are being processed .....	12
2.2.1.2	Access to the personal data being processed .....	12
2.2.1.3	Information on the processing and on data subject rights .....	13
2.2.2	Provisions on Modalities .....	13
2.2.2.1	Providing a copy .....	13
2.2.2.2	Providing further copies .....	14
2.2.2.3	Making the information available in a commonly used electronic form .....	15
2.2.3	Possible limitation of the right of access.....	15
2.3	General principles of the right of access.....	15
2.3.1	Completeness of the information .....	16
2.3.2	Correctness of the information .....	18
2.3.3	Time reference point of the assessment.....	18
2.3.4	Compliance with data security requirements .....	19
3	General considerations regarding the assessment of access requests.....	20
3.1	Introduction.....	20
3.1.1	Analysis of the content of the request .....	20
3.1.2	Form of the request.....	22
3.2	Identification and authentication.....	24
3.3	Proportionality assessment regarding authentication of the requesting person.....	26
3.4	Requests made via third parties / proxies.....	29
3.4.1	Exercise of the right of access on behalf of children.....	29
3.4.2	Exercising the right of access through portals / channels provided by a third party....	30
4	Scope of the right of access and the personal data and information to which it refers.....	31
4.1	Definition of personal data.....	31
4.2	The personal data the right of access refers to.....	34
4.2.1	“personal data concerning him or her”.....	34
4.2.2	Personal data which “are being processed” .....	36
4.2.3	The scope of a new request to access.....	37
4.3	Information on the processing and on data subject rights .....	37

5	How can a controller provide access? .....	41
5.1	How can the controller retrieve the requested data? .....	41
5.2	Appropriate measures for providing access.....	42
5.2.1	Taking “appropriate measures” .....	42
5.2.2	Different means to provide access.....	43
5.2.3	Providing access in a ”concise, transparent, intelligible and easily accessible form using clear and plain language” .....	44
5.2.4	A large quantity of information necessitates specific requirements on how the information is provided.....	46
5.2.5	Format .....	47
5.3	Timing for the provision of access.....	50
6	Limits and restrictions of the right of access.....	51
6.1	General remarks .....	51
6.2	Article 15 (4) GDPR .....	52
6.3	Article 12(5) GDPR .....	55
6.3.1	What does manifestly unfounded mean? .....	55
6.3.2	What does excessive mean? .....	56
6.3.3	Consequences.....	59
6.4	Possible restrictions in Union or Member States law based on Article 23 GDPR and derogations .....	60
	Annex – Flowchart.....	61

# The European Data Protection Board

Having regard to Article 70 (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"),

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<sup>1</sup>,

Having regard to Article 12 and Article 22 of its Rules of Procedure,

Whereas the preparatory work of these guidelines involved the collection of inputs from stakeholders, both in writing and at a dedicated stakeholders event on data subject rights, in order to identify the challenges and interpretation issues faced in the application of the relevant provisions of the GDPR;

## HAS ADOPTED THE FOLLOWING GUIDELINES

### 1 INTRODUCTION - GENERAL OBSERVATIONS

1. In today's society, personal data are processed by public and private entities, during many activities, for a wide array of purposes and in many different ways. Individuals may often be in a disadvantaged position in terms of understanding how their personal data are processed, including the technology used in the particular case, whether it is by a private or a public entity. In order to protect personal data of natural persons in these situations, the GDPR has created a coherent and robust legal framework, generally applicable with regard to different types of processing, including specific provisions relating to data subject rights.
2. The right of access to personal data is one of the data subjects' rights provided for in Chapter III of the GDPR among other rights, such as for instance the right to rectification and erasure, the right to restriction of processing, the right to portability, the right to object or the right of not being subject to automated individual decision making, including profiling<sup>2</sup>. The right of access by the data subject is enshrined both in the Charter of Fundamental Rights of the EU (the Charter)<sup>3</sup> and in Art. 15 GDPR, where it is precisely formulated as the right of access to personal data and to other related information.
3. Under the GDPR, the right of access consists of three components i.e. confirmation of whether or not personal data are processed, access to it, and information about the processing itself. The data subject can also obtain a copy of the processed personal data, whereas this possibility is not an additional data subject right but the modality of providing access to the data. Thus, the right of access can be understood both as the possibility of the data subject to ask the controller if personal data about him or her are processed and as the possibility to access and to verify these data. The controller shall

---

<sup>1</sup> References to "Member States" made throughout this document should be understood as references to "EEA Member States".

<sup>2</sup> Art. 15 - 22 GDPR.

<sup>3</sup> Under Art. 8 para. 1 of the Charter of Fundamental Rights of the European Union Everyone has the right to the protection of personal data concerning him or her. Under Art. 8 para. 2 sentence 2 Everyone has the right of access to data which has been collected concerning him or her and the right to have it rectified.

provide to the data subject, on the basis of his/her request, the information falling within the scope of Art. 15(1) and (2) GDPR.

4. The exercise of the right of access is realised both in the framework of data protection law, in accordance with the objectives of data protection law, and more specifically, in the framework of "*fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data*", as put forward by Art. 1(2) GDPR. The right of access is an important element of the whole data protection system.
5. The practical aim of the right of access is to enable the natural persons to have the control over their own personal data<sup>4</sup>. In order to realise this goal effectively in practice, the GDPR is aiming to facilitate this exercise by number of guarantees enabling the data subject to exercise this right easily, without unnecessary constraints, at reasonable intervals and without excessive delay or expense. All this should lead to more effective enforcement of the right of access by data subject in the digital age, part of which in a broader sense is also the data subject's right to file a complaint to the supervisory authority and the right to effective judicial protection<sup>5</sup>.
6. With regards to the development of the right of access, as part of the data protection legal framework, it should be stressed that it has been an element of the European data protection system from its beginning. In comparison with Directive 95/46/EC, the standard of the data subject rights set out in the GDPR has been both refined and strengthened; this also applies to the right of access. As the modalities of the right of access are now specified more precisely in the GDPR, this right is also more instructive from the point of legal certainty for both the data subject and the controller. Besides, the specific wording of Art. 15, and the precise deadline for the provision of data under Art. 12(3) GDPR, obliges the controller to be prepared for data subject inquiries by developing procedures for handling requests.
7. The right of access should not be seen in isolation as it is closely linked with other provisions of the GDPR, in particular with data protection principles including the fairness and lawfulness of processing, the controller's transparency obligation and with other data subject rights provided for in Chapter III of the GDPR.
8. In the framework of data subject rights, it is also important both to stress the significance of Art. 12 GDPR, which lays down requirements for appropriate measures adopted by the controller in providing the information referred to in Art. 13 and 14 GDPR, and the communications referred to in Art. 15-22 and 34 GDPR; these requirements generally specify the form, manner and time limit for the responses to the data subject, and in particular for any information addressed to the child.
9. The EDPB considers it necessary to provide more precise guidance on how the right of access has to be implemented in different situations. These guidelines aim at analysing the various aspects of the right of access. More particularly, the section hereafter is meant to give a general overview and explanation of the content of the Art. 15 itself whereas the subsequent sections provide deeper analysis of the most frequent practical questions and issues concerning the implementation of the right of access.

---

<sup>4</sup> See recitals 7, 68, 75 and 85 of the GDPR

<sup>5</sup> See Chapter VIII Articles 77, 78 and 79 of the GDPR

## 2 AIM OF THE RIGHT OF ACCESS, STRUCTURE OF ARTICLE 15 GDPR AND GENERAL PRINCIPLES

### 2.1 Aim of the right of access

10. The right of access is thus designed to enable natural persons to have control over personal data relating to them in that it allows them, “*to be aware of, and verify, the lawfulness of the processing*”<sup>6</sup>. More specifically, the purpose of the right of access is to make it possible for the data subjects to understand how their personal data are being processed as well as the consequences of such processing, and to verify the accuracy of the data processed without having to justify their intention. In other words, the purpose of the right of access is to provide individuals with sufficient, transparent and easily accessible information about data processing, regardless of the technologies used, and to enable them to verify different aspects of a particular processing activity under the GDPR (e.g. lawfulness, accuracy).
11. The interpretation of the GDPR provided in these guidelines is based on the CJEU case law which has been rendered so far. Taking into account the importance of the right of access, related case law can be expected to evolve significantly in future.
12. In accordance with CJEU decisions<sup>7</sup>, the right of access serves the purpose of guaranteeing the protection of the data subjects’ right to privacy and data protection with regard to the processing of data relating to them<sup>8</sup> and may facilitate the exercise of their rights flowing from, for example, Art. 16 to 19, 21 to 22 and 82 GDPR. However, the exercise of the right of access is an individual’s right and not conditional upon the exercise of those other rights and the exercise of the other rights does not depend on the exercise of the right of access.
13. Given the broad aim of the right of access, the aim of the right of access is not suitable to be analysed as a precondition for the exercise of the right of access by the controller as part of its assessment of access requests. Thus, controllers should not assess “why” the data subject is requesting access, but only “what” the data subject is requesting (see section 3 on the analysis of the request) and whether they hold personal data relating to that individual (see section 4). Therefore, for example, the controller should not deny access on the grounds or the suspicion that the requested data could be used by the data subject to defend themselves in court in the event of a dismissal or a commercial dispute with the controller.<sup>9</sup> Regarding limits and restrictions of the right of access, please see section 6.

**Example 1:** An employer dismissed an individual. One week later, the individual decides to collect evidence to file an unfair dismissal lawsuit against this former employer. With that in mind, the individual writes to the former employer requesting access to all personal data relating to him or her, as data subject, that the former employer, as controller, processes.

The controller shall not assess the intention of the data subject, and the data subject does not need to provide the controller with the reason for the request. Therefore, if the request fulfils all other requirements (see section 3), the controller needs to comply with the request, unless the request

<sup>6</sup> Recital 63 GDPR.

<sup>7</sup> CJEU, C-434/16, Nowak, and joined cases C-141/12 and C-372/12, YS and Others.

<sup>8</sup> CJEU, C-434/16, Nowak, para. 56.

<sup>9</sup> Questions related to this topic are at issue in a case currently pending before the CJEU (C-307/22).

proves to be manifestly unfounded or excessive in accordance with Art. 12 (5) of the GDPR (see section 6.3), which the controller is required to demonstrate.

**Variation:** The data subject exercises the right of access with regard to the personal data relating to him or her during the course of the lawsuit. However, the national law of the Member State, which governs the employment relation between the controller and the data subject, contains certain provisions that limit the scope of information to be provided to or exchanged between parties to ongoing or prospective legal proceedings, which are applicable to the unfair dismissal lawsuit that the data subject filed. In this context and provided that, these national provisions comply with the requirements posed by Art. 23 GDPR<sup>10</sup>, the data subject is not entitled to receive more information from the controller than is prescribed by the national law provisions of the Member State governing the information exchange between parties to legal disputes.

14. Although the aim of the right of access is broad, the CJEU illustrated also the limits of the remit of data protection law and the right of access. For instance, the CJEU found that the objective of the right of access guaranteed by EU data protection law is to be distinguished from that of the right of access to public documents established by EU and national legislation, the latter aiming at, “the greatest possible transparency of the decision-making process of the public authorities and to promote good administrative practices”<sup>11</sup>, an objective not sought by data protection law. The CJEU concluded that the right of access to personal data applies irrespective of whether a different kind of right of access with a different aim applies, such as in the context of an examination procedure.

## 2.2 Structure of Article 15 GDPR

15. In order to reply to a request for access and to ensure that none of its aspects might be disregarded, it is necessary first to understand the structure of Art. 15 and the constituent components of the right of access stipulated in this Article.
16. Art. 15 can be broken down into eight different elements as listed in the table below:

1.	Confirmation as to whether or not the controller is processing personal data concerning the requesting person	Art. 15(1), first half of the sentence
2.	Access to the personal data concerning the requesting person	Art. 15(1), second half of the sentence (first part)
3.	Access to the following information on the processing: (a) the purposes of the processing; (b) the categories of personal data; (c) the recipients or categories of recipients; (d) the envisaged duration of the processing or the criteria for determining the duration; (e) the existence of the rights to rectification, erasure, restriction of processing and objection to processing; (f) the right to lodge a complaint with a supervisory authority; (g) any available information on the source of the data, if not collected from the data subject;	Art. 15(1), second half of the sentence (second part)

<sup>10</sup> EDPB Guidelines 10/2020 on restrictions under article 23 GDPR, version for public consultation, 18 December 2020.

<sup>11</sup> CJEU, Joined cases C-141/12 and C-372/12, YS and Others, para. 47.

	(h) the existence of automated decision-making, including profiling and other information relating thereto.	
4.	Information on safeguards pursuant to Art. 46 where the personal data are transferred to a third country or to an international organisation	Art. 15(2)
5.	The obligation of the controller to provide a copy of the personal data undergoing processing	Art. 15(3), first sentence
6.	Charging of a reasonable fee by the controller based on administrative costs for any further copies requested by the data subject	Art. 15(3), second sentence
7.	Provision of information in electronic form	Art. 15(3), third sentence
8.	Taking into account the rights and freedoms of others	Art. 15(4)

While all elements of Art. 15(1) and (2) together define the content of the right of access, Art. 15(3) deals with the modalities of access, in addition to the general requirements set out in Art. 12 GDPR. Art. 15(4) supplements the limits and restrictions that Art. 12(5) GDPR provides for all data subjects' rights with a specific focus on rights and freedoms of others in the context of access.

## 2.2.1 Defining the content of the right of access

17. Art. 15(1) and (2) contain the following three aspects: first, the confirmation whether personal data of the requesting person are being processed, if yes, second, access to those data, and, third, information on the processing. They can be regarded as three different components which together build the right of access.

### 2.2.1.1 Confirmation as to 'whether' or not personal data are being processed

18. When making a request for access to personal data, the first thing that the data subjects need to know is whether or not the controller processes data concerning them. Consequently, this information constitutes the first component of the right of access under Art. 15(1). Where the controller does not process personal data relating to the data subject requesting the access, the information to be provided would be limited to confirming that no personal data relating to the data subject are being processed. Where the controller does process data relating to the requesting person, the controller must confirm this fact to this person. This confirmation may be communicated separately, or it may be encompassed as part of the information on the personal data being processed (see below).

### 2.2.1.2 Access to the personal data being processed

19. Access to personal data is the second component of the right of access under Art. 15(1) and it constitutes the core of this right. It relates to the notion of personal data as defined by Art. 4(1) GDPR. Aside from basic personal data like name and address, an unlimited variety of data may fall within this definition, provided that they fall under the material scope of the GDPR, notably with regards to the way in which there are processed (Art. 2 GDPR). Access to personal data hereby means access to the actual personal data themselves, not only a general description of the data nor a mere reference to the categories of personal data processed by the controller. If no limits or restrictions apply<sup>12</sup>, data subjects are entitled to have access to all data processed relating to them, or to parts of the data,

---

<sup>12</sup> See section 6 of these Guidelines.

depending on the scope of the request (see sec. 2.3.1). The obligation to provide access to the data does not depend on the type or source of those data. It applies to its full extent even in cases where the requesting person had initially provided the controller with the data, because its aim is to let the data subject know about the actual processing of those data by the controller. The scope of personal data under Art. 15 is explained in detail in sec. 4.1 and 4.2.

#### 2.2.1.3 Information on the processing and on data subject rights

20. The third component of the right of access is the information on the processing and on data subjects' rights that the controller has to provide under Art. 15(1)(a) to (h) and 15(2). Such information could be based on text taken, for example, from the privacy notice of the controller<sup>13</sup> or from the controller's record of processing activities referred to in Art. 30 GDPR, but may have to be updated and tailored to the data subject's request. The content and degree of specification of the information is further elaborated in section 4.3.

#### 2.2.2 Provisions on Modalities

21. Art. 15(3) supplements the requirements for the modalities of the reply to access requests laid down in Art. 12 GDPR by some specifications in context of access requests.

##### 2.2.2.1 Providing a copy

22. Under the first sentence of Art. 15(3) GDPR, the controller shall provide a free copy of the personal data which the processing relates to. The copy therefore refers only to the second component of the right of access («access to the personal data processed», see above). The controller must ensure that the first copy is free of charge, even where it considers the cost of reproduction to be high (example: the cost of providing a copy of the recording of a telephone conversation).
23. The obligation to provide a copy is not to be understood as an additional right of the data subject, but as modality of providing access to the data. It strengthens the right of access to the data<sup>14</sup> and helps to interpret this right because it makes clear, that access to the data under Art. 15(1) comprises complete information on all data and cannot be understood as granting only a summary of the data. At the same time, the obligation to provide a copy is not designed to widen the scope of the right of access: it refers (only) to a copy of the personal data undergoing processing, not necessarily to a reproduction of the original documents (see section 5, para. 152). More generally speaking, there is no additional information to be given to the data subject upon providing a copy: the scope of the information to be contained in the copy is the scope of the access to the data under 15(1) (second component of the right of access as referred to above, see para. 19), which includes all information necessary to enable the data subject to understand and verify the lawfulness of the processing.<sup>15</sup>
24. In light of the above, if access to the data in the sense of Art. 15(1) is given by providing a copy, the obligation to provide a copy mentioned under 15(3) is complied with. The obligation to provide a copy serves the objectives of the right of access to allow the data subject to be aware of, and verify the lawfulness of the processing (Recital 63). To achieve these objectives, the data subject will in most

---

<sup>13</sup> See for information on this Art. 29 Working Party, WP260 rev.01, 11 April 2018, Guidelines on transparency under Regulation 2016/679 - endorsed by the EDPB (hereinafter "WP29 Guidelines on transparency - endorsed by the EDPB").

<sup>14</sup> The obligation to provide a copy was not mentioned in the Data Protection Directive 95/46/EC.

<sup>15</sup> Questions related to the topic of this paragraph are at issue in a case currently pending before the CJEU (C-487/21

cases need to see the information not only temporarily. Therefore, the data subject will need to get access to the information by receiving a copy of the personal data.

25. In view of the above, the notion of a copy has to be interpreted in a broad sense and includes the different kinds of access to personal data as long as it is complete (i.e. it includes all personal data requested) and possible for the data subject to keep. Thus, the requirement to provide a copy means, that the information on the personal data concerning the person who makes the request is provided to the data subject in a way which allows the data subject to retain all of the information and to come back to it.
26. In spite of this broad understanding of a copy, and regarding that it is the main modality by which access should be provided, under some circumstances other modalities could be appropriate. Further explanations on copies and other modalities of providing access are given in section 5, in particular 5.2.2 - 5.2.5.

#### [2.2.2.2 Providing further copies](#)

27. Art. 15(3), second sentence concerns situations where the data subject asks the controller for more than one copy, for example in case the first copy was lost or damaged or the data subject wants to pass on a copy to another person or a Supervisory Authority. On the basis that further copies must be provided by the controller upon request of the data subject, Art. 15(3) rules, that for any further copy requested, the controller may charge a reasonable fee based on administrative costs (Art. 15(3) second sentence).
28. If the data subject asks for an additional copy after the first request was made, questions may arise on whether this should be regarded as a new request, or whether the data subject wants an additional copy of the data in the sense of Art. 15(3) second sentence, in which case a fee for an additional copy may be charged. The response to these questions depends solely on the content of the request: the request should be interpreted as asking for an additional copy, insofar as, in terms of time and scope, it concerns the same processing of personal data as the former request. If, however, the data subject aims to get information on the data processed at a different point in time or relating to a different set of data from the one initially requested, the right to obtain a free copy according to Art. 15(3), applies once again. This also is valid in cases where the data subject has made a first request shortly beforehand. A data subject may exercise its right of access through a subsequent request and obtain a free copy, unless the request is regarded as excessive under Art. 12(5) with the possibility of charging a reasonable fee in accordance with Art. 12(5)(a) (on excessive character of repetitive requests, see section 6).

**Example 2:** A customer submits an access request to a trading company. One year after the reply of the company, the same customer makes a request for access under Art. 15 to the same company. Irrespective of whether there have been new business transactions or other contacts between the parties since the previous request, this second request is to be regarded as a new request. Even if no change in the data processing by the company occurred – which is not necessarily apparent to the data subject – the data subject has the right to get a free copy of the data.

**Variation 1:** Even if the customer in the above cases places the new request for example only one week after the first request, this may well be regarded as a new request under Art. 15(1) and (3), first sentence, if it is not to be interpreted as a mere reminder of the first request. Regarding the short interval and depending on the specific circumstances of the new request, its excessiveness according to Art. 12(5) is at issue (see section 6).

**Variation 2:** The request for a “new copy” of the information that had already been given in form of a copy in response to a previous request, for example in case that the customer lost the copy previously received, should, as a matter of course, be regarded as a request for an additional copy as it refers to the previous request in scope and time of the processing.

29. If the data subject repeats a first request for access on the grounds that the answer received was not complete or that no reasons had been given for the refusal, this request is not to be regarded as a new request, since it is merely a reminder of a first unsatisfied request.
30. Concerning the allocation of costs in cases of requests for an additional copy, Art. 15(3) establishes that the controller may charge a reasonable fee based on the administrative costs that are caused by the request. This means, that the administrative costs are a relevant criterion for fixing the level of the fee. At the same time, the fee should be appropriate, taking into account the importance of the right of access as a fundamental right of the data subject. The controller should not pass on overhead costs or other general expenses to the data subject, but should focus on the specific costs that were caused by providing the additional copy. When organising this process the controller should deploy its human and material resources efficiently in order to keep the costs of the copy low, including if the controller involves external support.
31. In case the controller decides to charge a fee, the controller should indicate in advance that a fee will be charged and – as accurately as is possible - the amount of costs it is planning to charge to the data subject in order to give the data subject the possibility to determine whether to maintain or to withdraw the request.

#### 2.2.2.3 Making the information available in a commonly used electronic form

32. In the event of a request by electronic form means, information shall be provided by electronic means where possible and unless otherwise requested by the data subject (see Art. 12(3) GDPR). Art. 15(3), third sentence, complements this requirement in the context of access requests by stating, that the controller is in addition obliged to provide the answer in a commonly used electronic form, unless otherwise requested by the data subject. Art. 15(3) presupposes, that for controllers who are able to receive electronic requests it will be possible to provide the reply to the request in a commonly used electronic form (for details see sec. 5.2.5). This provision refers to all the information that needs to be provided in accordance with Art. 15(1) and (2). Therefore, if the data subject submits the request for access by electronic means, all information must be provided in a commonly used electronic form. Questions of format are further developed in section 5. The controller should, as always, deploy appropriate security measures, in particular when dealing with special category of personal data (see below, under 2.3.4 ).

#### 2.2.3 Possible limitation of the right of access

33. Finally, in context of the right of access, a specific limitation is foreseen in Art. 15(4). It states, that possible adverse effects on the rights and freedoms of others have to be considered. Questions as to the scope and the consequences of this limitation as well as to additional limits and restrictions set forth in Art. 12(5) GDPR or under Art. 23 GDPR are explained in section 6.

### 2.3 General principles of the right of access

34. When data subjects make a request for access to their data, in principle, the information referred to in Art. 15 GDPR must always be provided in full. Accordingly, where the controller processes data relating to the data subject, the controller shall provide all the information referred to in Art. 15(1)

and, where applicable, the information referred to in Art. 15(2). The controller has to take the appropriate measures to ensure that the information is complete, correct and up-to-date, corresponding as close as possible to the state of data processing at the time of receiving the request<sup>16</sup>. Where two or more controllers process data jointly, the arrangement of the joint controllers regarding their respective responsibilities with regards to the exercise of data subject's rights, especially concerning the answer to access requests, does not affect the rights of the data subjects towards the controller to whom they address their request<sup>17</sup>.

### 2.3.1 Completeness of the information

35. Data subjects have the right to obtain, with the exceptions mentioned below, full disclosure of all data relating to them (for details on the scope, see section 4.2). Unless explicitly requested otherwise by the data subject, a request to exercise the right of access shall be understood in general terms, encompassing all personal data concerning the data subject<sup>18</sup>. Limiting access to part of the information may be considered in the following cases:
- a) The data subject has explicitly limited the request to a subset. In order to avoid providing incomplete information, the controller may consider this limitation of the data subject's request only if it can be certain that this interpretation corresponds to the wish of the data subject (for further details, see section 3.1.1, para. 51). In principle, the data subject shall not have to repeat the request for the transmission of all the data the data subject is entitled to obtain.
  - b) In situations where the controller processes a large quantity of data concerning the data subject, the controller may have doubts if a request of access, that is expressed in very general terms, really aims at receiving information on all kind of data being processed or on all branches of activity of the controller in detail. These may arise in particular in situations, where there was no possibility to provide the data subject with tools to specify their request from the beginning or where the data subject did not make use of them. The controller then faces problems of how to give a full answer while simultaneously avoiding the creation of an overflow of information for the data subject that the data subject is not interested in and cannot effectively handle. There may be ways to solve this problem, depending on the circumstances and the technical possibilities, for example by providing self-service tools in online contexts (see section 5 on the layered approach). If such solutions are not applicable, a controller who processes a large quantity of information relating to the data subject may request the data subject to specify the information or processing to which the request relates before the information is delivered (see Recital 63 GDPR). Examples of this may include a company with several fields of activity or a public authority with different administrative units, if the controller found that numerous data relating to the data subject are processed in those branches. In addition, a large quantity of data may be processed by controllers who collect data regarding frequent activities of the data subject over a prolonged time period.

**Example 3:** A public authority processes data on the data subject in a number of different departments concerning various contexts. File management and file keeping are partly processed by non-automated means and most of the data is only stored in paper files. Regarding the general wording of the request, the public authority doubts whether the data subject is aware of the extent

---

<sup>16</sup> For guidance on appropriate measures see sec. 5 para. 123 - 129

<sup>17</sup> EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, par. 162f.. Processors have to assist the controller, ibd., para. 129.

<sup>18</sup> For details please see section 5.2.3 below on the topic of layered approach.

of the request, especially the variety of processing operations that it would encompass, the amount of information and the number of pages that the data subject would receive.

**Example 4:** A big insurance company receives a general access request by letter from a person who has been a customer for many years. Even though deletion periods are fully respected, the company actually processes a vast amount of data concerning the customer, because processing is still necessary to fulfil contractual obligations arising from the contractual relationship with the customer (including for example continuing obligations, communication on controversial issues with the customer and with third parties, ...) or to comply with legal obligations (archived data that have to be stored for tax purposes, etc.). The insurance company may have doubts as to whether the request, that was made in very general terms, is really intended to encompass all kinds of those data. This may be especially problematic if the insurance company only has a postal address of the data subject and therefore has to send any information on paper. However, the same doubts may be relevant also when providing the information by other means.

If, in such cases, the controller decides to ask the data subject to specify the request, in order to fulfil its obligation to facilitate the exercise of the right of access (Art. 12(2) GDPR) the controller shall at the same time give meaningful information about its processing operations that could concern the data subject, by informing about relevant branches of its activities, databases etc.

**Example 5:** In an employment relationship, in case of a generally formulated request for access, it is not *per se* clear that the employee wants to receive all user-login data, data on access to a workplace, data on settlements in the canteen, data on salary payments, etc. A request for specification made by the employer could for example lead to the clarification, that the employee's interest is to understand or verify to whom his performance assessment has been passed on. Without request for specification, the employee would receive a large quantity of information, without having an interest in most of the data. At the same time, the employer would need to give information on the different contexts of processing which could concern the employee in order to allow the employee to specify the request sensibly.

It is important to underline that the request for specification shall not aim at a limitation of the reply to the access request and shall not be used to hide any information on the data or the processing concerning the data subject. If the data subject, who has been asked to specify the scope of its request, confirms to seek all personal data concerning him or her, the controller of course has to provide it in full.

In any case, the controller should always be able to demonstrate, that the way to handle the request aims to give the broadest effect to the right of access and that it is in line with its obligation to facilitate the exercise of data subjects rights (Art. 12(2) GDPR). Subject to these principles, the controller may await the answer of the data subject before providing additional data according to the data subject's wish, if the controller has provided the data subject with a clear overview of all processing operations that could concern the data subject, including especially those that the data subject might not have expected, if the controller has also given access to all data that the data subject clearly aimed for, and if, furthermore, this information has been combined with clear indication of how to get access to the remaining parts of the processed data.

- c) Exceptions or restrictions to the right of access apply (see below in section 6). In such cases, the controller should carefully check to which parts of the information the exception relates to and provide all information that is not excluded by the exception. For example, confirmation of the processing of personal data itself (component 1) may not be affected by the exception. As a result, information has

to be provided about all the personal data and all the information referred to in Art. 15(1) and (2) that are not concerned by the exception or the restriction.

### 2.3.2 Correctness of the information

36. The information included in the copy of the personal data given to the data subject has to comprise the actual information or personal data held about the data subject. This includes the obligation to give information about data that are inaccurate or about data processing which is not or no longer lawful. The data subject may for example use the right of access to find out about the source of inaccurate data being circulated between different controllers. If the controller corrected inaccurate data before informing the data subject about it, the data subject would be deprived of this possibility. The same applies in case of unlawful processing. The possibility to know about unlawful processing concerning the data subject is one of the main purposes of the right of access. The obligation to inform about the unchanged state of processing is without prejudice to the obligation of the controller to end unlawful processing or to correct inaccurate data. Questions about the order in which those obligations should be fulfilled, are answered in the following.

### 2.3.3 Time reference point of the assessment

37. The assessment of the data being processed shall reflect as close as possible the situation when the controller receives the request and the response should cover all data available at that point in time. This means that the controller has to try to find out about all the data processing activities relating to the data subject without undue delay. Controllers are thus not required to provide personal data, which they processed in the past but which they no longer have at their disposal<sup>19</sup>. For instance, the controller may have deleted personal data in accordance with its data retention policy and/or statutory provisions and may thus no longer be able to provide the requested personal data. In this context, it should be recalled that the length of time for which the data are stored should be fixed in accordance with Art. 5(1)(e) GDPR, as any retention of data must be objectively justifiable.
38. At the same time, the controller shall implement in advance the necessary measures in order to facilitate the exercise of the right of access and to deal with such requests as soon as possible (see Art. 12(3)) and before the data will have to be deleted. Therefore, in the case of short retention periods, the measures taken to answer the request should be adapted to the appropriate retention period in order to facilitate the exercise of the right of access and to avoid the permanent impossibility of providing access to the data processed at the moment of the request<sup>20</sup>. In some cases it may nevertheless not be possible to reply to a request before the time the data are scheduled for deletion. For example, if in course of replying to a request as promptly as possible, a controller retrieves personal data that were scheduled to be deleted the following day, the controller may need some additional time to consider whether redactions need to be made to protect the freedoms of others before releasing a copy of the personal data to the requester. If the data have been retrieved within the

---

<sup>19</sup> See, to that effect, further clarifications in section 4 of these guidelines, as well as in Court of Justice of the European Union, C-553/07, 7 May 2009, *College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer* on a right of access to information on the recipients or categories of recipients in respect of the past.

<sup>20</sup> For example, the implementation of a self-service tool enabling the data subject to easily access the requested personal data and a notification system alerting the controller about a request that relates to personal data with short retention periods could be considered in order to facilitate prompt action.

scheduled retention period, the controller may continue to process those data for the purpose to fulfill its obligation to answer the request. Processing in such cases may be based on Art. 6(1)(c) in combination with Article 15 GDPR and its duration has to comply with the requirements of Art. 12(3) GDPR<sup>21</sup>. The application of this legal basis is limited to processing of the data identified to be necessary for answering the concrete request and is not to be used as a justification for general extenions of retention periods.

39. Furthermore, the controller shall not deliberately escape the obligation to provide the requested personal data by erasing or modifying personal data in response to a request for access (see 2.3.2). If, in the course of processing the access request, the controller discovers inaccurate data or unlawful processing, the controller has to assess the state of the processing and to inform the data subject accordingly before complying with its other obligations. In its own interest, to avoid the need of further communication on this as well as to be compliant with the transparency principle, the controller should add information about the subsequent rectifications or deletions.

**Example 6:** On the occasion of replying to an access request a controller realises, that an application of the data subject for a vacancy in the company of the controller has been stored beyond the retention period. In this case the controller cannot delete first and then reply to the data subject that no data (concerning the application) is processed. It has to give access first and delete the data afterwards. In order to prevent a subsequent request for erasure it would then be recommended to add information about the fact and time of the deletion.

In order to comply with the principle of transparency, controllers should infom the data subject as of the specific point in time of the processing to which the response of the controller refers. In some cases, for example in contexts of frequent communication activities, additional processing or modifications of the data may occur between this time reference point, at which the processing was assessed, and the response of the controller. If the controller is aware of such changes, it is recommended to include information about those changes as well as information about additional processing necessary to reply to the request.

#### 2.3.4 Compliance with data security requirements

40. Since communicating and making available personal data to the data subject is a processing operation, the controller is always obliged to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing (see Art. 5(1)(f), 24 and 32 GDPR). This applies independently of the modality in which access is provided. In case of non-electronic transmission of the data to the data subject, depending on the risks that are presented by the processing, the controller may consider using registered mail or, alternatively, to offer, but not oblige, the data subject to collect the file against signature directly from one of the controller's establishments. If, in line with Art. 12(1) and (3), information is provided by electronic means, the controller shall choose electronic means that comply with data security requirements. Also in case of providing a copy of the data in a commonly used electronic form (see Art. 15(3)), the controller shall take into account data security requirements when choosing the means of how to transmit the electronic file to the data subject. This may include applying encryption, password protection etc. In order to facilitate access to the encrypted data, the controller should also ensure that appropriate information is made available so that the data subject can access the decrypted information. In cases

---

<sup>21</sup> This is without prejudice to subsequent processing of data for evidence purposes in connection with the handling of the access request for an appropriate period of time.

where data security requirements would necessitate end-to-end encryption of electronic mails but the controller would only be able to send a normal e-mail, the controller will have to use other means, such as sending a USB-stick by (registered) letter post to the data subject.

### 3 GENERAL CONSIDERATIONS REGARDING THE ASSESSMENT OF ACCESS REQUESTS

#### 3.1 Introduction

41. When receiving requests for access to personal data, the controller must assess each request individually. The controller shall take into consideration, *inter alia*, the following issues, further developed in the following paragraphs: whether the request concerns personal data linked to the requesting person and who the requesting person is. This section aims to clarify what elements of the request for access the controller should take into account when carrying out its assessment and to discuss possible scenarios for such an assessment as well as its consequences. The controller, when assessing a request for access to personal data, shall also take into account, pursuant to Art. 12(2) GDPR, the obligation to facilitate the exercise of the data subject rights, while keeping in mind the appropriate security of the personal data<sup>22</sup>.
42. Therefore, the controllers should be proactively ready to handle the requests for access to personal data. This means that the controller should be prepared to receive the request, assess it properly (this assessment is the subject of this section of the guidelines) and provide an appropriate reply without undue delay to the requesting person. The way the controllers will prepare themselves for the exercise of access requests should be adequate and proportionate and depend on the nature, scope, context and purposes of processing as well as the risks to the rights and freedoms of natural persons, in accordance with Art. 24 GDPR. Depending on the particular circumstances, the controllers may, for example, be required to implement an appropriate procedure, the implementation of which should guarantee the security of the data without hindering the exercise of the data subject's rights.

##### 3.1.1 Analysis of the content of the request

43. This issue can be more specifically assessed by asking the following questions.
  - a) Does the request concern personal data?
44. Under the GDPR, the scope of the request shall only cover personal data<sup>23</sup>. Therefore, any request for information about other issues, including general information about the controller, its business models or its processing activities not related to personal data, is not to be considered as a request made pursuant to Art. 15 GDPR. Additionally, a request for information about anonymous data or data that

---

<sup>22</sup> The controller shall ensure appropriate security of the personal data, in accordance with the integrity and confidentiality principle (Art. 5(1)(f) GDPR), by implementing appropriate technical and organisational measures, as referred to in Art. 32 GDPR and elaborated in Art. 24 GDPR. The controller shall be able to demonstrate that it ensures an adequate level of data protection, in line with the accountability principle (see also: Art. 29 Working Party Opinion 3/2010 on the principle of accountability adopted on 13 July 2010, 00062/10/EN WP 173 and EDPB Guidelines nr 07/2020 on the concepts of controller and processor in the GDPR).

<sup>23</sup> Unless the request covers also non-personal data inextricably linked to the personal data of the data subject. For further explanations see para 100.

does not concern the requesting person or the person on whose behalf the authorised person made the request, will not be within the scope of the right of access. This question will be analysed more in detail in section 4.

45. Unlike anonymous data (which are not personal data), pseudonymised data, which could be attributed to a natural person by the use of additional information, are personal data<sup>24</sup>. Thus, pseudonymised data that can be linked to a data subject - e.g. when the data subject provides the respective identifier allowing their identification, or when the controller is able to connect the data to the requesting person by its own means - are to be considered within the scope of the request<sup>25</sup>.

b) Does the request relate to the requesting person (or the person on whose behalf the authorised person makes the request)?

46. As a general rule, a request may only concern the data of the person making the request. Access to other people's data can only be requested subject to appropriate authorisation<sup>26</sup>.

**Example 7:** Data subject X works as a department manager for a company that provides parking spaces for its managers at a company car park. Although data subject X has a permanent parking space, when the data subject arrives at the office for their second shift, this space is often already occupied by another car. Since this situation is repetitive, in order to identify the driver who unauthorised occupies its slot, the data subject asks the controller of the video surveillance system covering the office's parking lot area, for access to the personal data of this driver. In such a case, data subject X's request will not be a request for access to their personal data, as the request does not concern the requesting person's data, but the data of another person - and therefore it should not be considered a request under Art. 15 GDPR.

c) Do provisions, other than the GDPR, regulating access to a certain category of data apply?

47. Data subjects are not required to specify the legal basis in their request. However, if the data subjects clarify that their request is based on sectoral legislation or on national legislation regulating the specific issue of access to certain categories of data, and not on the GDPR, such a request shall be examined by the controller in accordance with such sectoral or national rules, where applicable. Often, depending on the relevant national legislation, controllers may be required to provide separate replies, each dealing with the specific requirements set out by the different legislative acts. This is not to be confused with national or EU legislation setting out restrictions on the right of access which needs to be complied with when answering access requests.
48. If the controller has doubts as to which right the data subject wishes to exercise, it is recommended to ask the data subject making the request to explain the subject matter of the request. Such correspondence with the data subject shall not affect the duty of the controller to act without undue delay<sup>27</sup>. However, in case of doubts, if the controller asks the data subject for further explanation and receives no response, bearing in mind the obligation to facilitate the exercise of the person's right of access, the controller should interpret the information contained in the first request and act on this basis. In accordance with the accountability principle, the controller may determine an appropriate

---

<sup>24</sup> See Recital 26 GDPR. Further explanations on the concepts of anonymous data and pseudonymised data can be found in WP29 Opinion 4/2007 on the concept of personal data, p. 18-21.

<sup>25</sup> Art. 29 Working Party, WP242 rev.01, 5 April 2017, Guidelines on the right to data portability - endorsed by the EDPB (hereinafter "WP29 Guidelines on the right to data portability - endorsed by the EDPB"), p. 9.

<sup>26</sup> See section 3.4 ("Requests made via third parties/proxies").

<sup>27</sup> See further guidance on the timing in section 5.3.

timeframe during which the data subject may provide further explanation. When fixing such timeframe, the controller should leave enough time to comply with the request after it elapsed and therefore consider how much time is objectively necessary to compile and provide the requested data once the specification was provided (or not) by the data subject.

49. If the request is in the scope of the GDPR, the existence of such specific legislation does not override the general application of the right of access, as provided by the GDPR. There might be restrictions set out by EU or national law, when allowed by Art. 23 GDPR (see section 6.4).

*d) Does the request fall within the scope of Article 15?*

50. It should be noted that the GDPR does not introduce any formal requirements for persons requesting access to data. In order to make the access request, it is sufficient for the requesting persons to specify that they want to know what personal data concerning them the controller processes. Therefore, the controller cannot refuse to provide the data by referring to the lack of indication of the legal basis of the request, especially to the lack of a specific reference to the right of access or to the GDPR.

For example, in order to make a request, it would be sufficient for the requesting person to indicate that:

- they wish to obtain access to the personal data concerning them;
- they are exercising their right of access; or
- they wish to know the information concerning them that the controller processes.

It should be borne in mind that applicants may not be familiar with the intricacies of the GDPR and that it is advisable to be lenient towards persons exercising their right of access, in particular when it is exercised by minors. As indicated above, in case of any doubts it is recommended for the controller to ask the data subject making the request to specify the subject matter of the request.

*e) Do the data subjects want to access all or parts of the information processed about them?*

51. Additionally, the controller needs to assess whether the requests made by the requesting persons refer to all or parts of the information processed about them. Any limitation of the scope of a request to a specific provision of Art. 15 GDPR, made by the data subjects, must be clear and unambiguous. For example, if the data subjects require verbatim “information about the data processed in relation to them”, the controller should assume that the data subjects intend to exercise their full right under Art. 15(1) – (2) GDPR. Such a request should not be interpreted as meaning that the data subjects wish to receive only the categories of personal data that are being processed and to waive their right to receive the information listed in Art. 15(1)(a) to (h). This would be different, for example, where the data subjects wish, with regard to data which they specify, to have access to the source or origin of the personal data or to the specified period of storage. In such a case the controller may limit its reply to the specific information requested.

### 3.1.2 Form of the request

52. As noted previously, the GDPR does not impose any requirements on data subjects regarding the form of the request for access to the personal data. Therefore, there are, in principle, no requirements under the GDPR that the data subjects must observe when choosing a communication channel through which they enter into contact with the controller.

53. The EDPB encourages controllers to provide the most appropriate and user-friendly communication channels, in line with Art. 12(2) and Art. 25 GDPR, to enable the data subject to make an effective request. Nevertheless, if a data subject makes a request using a communication channel provided by the controller<sup>28</sup>, which is different from the one indicated as the preferable one, such request shall be, in general, considered effective and the controller should handle such a request accordingly (see the examples below). The controllers should undertake all reasonable efforts to make sure that the exercise of data subject rights is facilitated (for example, when a data subject sends an access request to an employee who is on leave, an automatic message informing the data subject about an alternative communication channel for this request could be a reasonable effort).
54. It should be noted that the controller is not obliged to act on a request sent to a random or incorrect e-mail (or postal) address, not directly provided by the controller, or to any communication channel that is clearly not intended to receive requests regarding data subject's rights if the controller has provided an appropriate communication channel, that can be used by the data subject.
55. The controller is also not obliged to act on a request sent to the e-mail address of a controller's employee who may not be involved in the processing of requests concerning data subjects' rights (e.g. drivers, cleaning staff, etc.). Such requests shall not be considered effective, if the controller has clearly provided the data subject with appropriate communication channel. However, if the data subject sends a request to the controller's employee who has been assigned to them as their regular contact person (such as e.g. a personal account manager at a bank or a regular consultant at a mobile phone operator), such contact should not to be considered as a random one and the controller should make all reasonable efforts, to handle such a request so that it can be redirected to the contact point and answered within the time limits provided for by the GDPR.
56. Nevertheless, the EDPB recommends, as good practice, that controllers introduce appropriate mechanisms to facilitate the exercise of data subjects' rights, including autoresponder systems to inform of staff absences and appropriate alternate contact and, where possible, mechanisms to improve internal communication between employees on requests received by those who may not be competent to deal with such requests.

**Example 8:** Controller C provides, both on its website and in the privacy notice, two e-mail addresses - the general e-mail address of the controller: CONTACT@C.COM and the e-mail address of the controller's data protection contact point: QUERIES@C.COM. Additionally, controller C indicates on its website that in order to submit any inquiries or to make a request with regard to the processing of personal data, individuals should contact the data protection contact point by way of the e-mail address provided. However, the data subject sends a request to the controller's general e-mail address: CONTACT@C.COM.

In such a case, the controller should make all reasonable efforts, to make its services aware of the request, which was made through the general e-mail, so that it can be redirected to the data protection contact point and answered within the time limits provided for by the GDPR. Moreover, the controller is not entitled to extend the period for responding to a request, merely because the data subject has

---

<sup>28</sup>This may include, for example, communication data of the controller provided in its communications addressed directly to data subjects or contact data provided by the controller publicly, such as in the controller's privacy policy or other mandatory legal notices of the controller (e.g. owner or business contact information on a website).

sent a request to the controller's general e-mail address, not the controller's data protection contact point e-mail address.

**Example 9:** Controller Y runs a network of fitness clubs. Controller Y indicates on its website and in the privacy notice for clients of the fitness club that in order to submit any inquiries or to make a request with regard to the processing of personal data, individuals should contact the controller under the e-mail address: QUERIES@Y.COM. Nevertheless, the data subject sends a request to an e-mail address found in the changing room, where he found a notice that reads "If you are not satisfied with the cleanliness of the room, please contact us at: CLEANERS@Y.COM", which is the e-mail address of the cleaning staff employed by Y. The cleaning staff are obviously not involved in handling matters concerning the exercise of the rights of data subjects - customers of the fitness club. Although the e-mail address was available on the premises of the fitness club, the data subject could not reasonably expect that this was an appropriate contact address for such requests, since the website and the privacy notice clearly informed about the communication channel to be used for the exercise of data subjects' rights.

57. Date of receipt of the request by the controller triggers, as a rule, the one month period for the controller to provide information on action taken on a request, in accordance with Art. 12(3) GDPR (further guidance on timing is provided in section 5.3). The EDPB considers as good practice for the controllers to confirm receipt of requests in writing, for example by sending e-mails (or information by post, if applicable) to the requesting persons confirming that their requests have been received and that the one month period runs from day X to day Y.

### 3.2 Identification and authentication

58. In order to ensure the security of processing and minimise the risk of unauthorised disclosure of personal data, the controller must be able to find out which data refer to the data subject (identification) and confirm the identity of that person (authentication).
59. It may be recalled that in situations in which the purpose for which the personal data are processed do not or no longer require the identification of a data subject, the controller does not need to maintain identification for the sole purpose of complying with data subjects' rights, also in light of the principle of data minimisation. These situations are dealt with in Art. 11(1) GDPR.
60. Art. 12(2) GDPR states that the controller shall not refuse to act on the request of the data subject to exercise his or her rights, unless the controller processes personal data for a purpose that does not require the identification of the data subject and it demonstrates that it is not in a position to identify the data subject. In such circumstances, the data subject may, however, decide to provide additional information enabling this identification (Art. 11(2) GDPR)<sup>29</sup>.
61. The controller is not obliged to acquire such additional information in order to identify the data subject for the sole purpose of complying with the data subject's request, also in light of the principle of data minimisation. However, it should not refuse to take such additional information provided by the data subject in order to support the exercise of his or her rights (Recital 57 GDPR).

**Example 10:** C is the controller of the data processed in connection with the video surveillance of a building. In accordance with Art. 11(1) GDPR, the controller is not obliged to identify all persons who

---

<sup>29</sup> WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 13.

have been registered by a security camera as a part of the monitoring (purpose not requiring identification). The controller receives a request for access to the personal data from the person who claims that to have been recorded by the controller's video surveillance. The controller's actions will depend on the additional information provided. If the requesting person indicates a particular day and time when the cameras may have recorded the event in question, it is likely that the controller will be able to provide such data (Art. 11(2) GDPR). However, if the controller is not in a position to identify the data subject (e.g. if it is impossible for the controller to be certain that a requesting person is in fact the data subject or if the request concerns e.g. a long period of recordings and a controller is unable to process such a large quantity of data), the controller may refuse to take action if it demonstrates that it is not in the position to identify the data subject (Art. 12(2) GDPR).

**Example 11:** A controller C processes personal data for the purpose of addressing behavioral advertising to its web users. Personal data collected for behavioral advertising are usually collected by means of cookies and associated with pseudonymous random identifiers. A data subject Mr. X exercises his right of access with C via C's website. C is able to precisely identify Mr. X to show the data subject's behavioral advertising, by linking the terminal equipment of Mr. X to its advertising profile with the cookies dropped in the terminal. C should then also be able to precisely identify Mr. X to grant him access to his personal data, as a link between the data processed and the data subject can be found. Therefore, and taking into account the principles of the GDPR, the above example would not fall within the scope of Art. 11 GDPR. More precisely, in the above example, the purposes of C require the identification of the data subjects while Art. 11 GDPR addresses the situation of processing which does not require identification where a controller shall not be obliged to process additional data within the meaning of Art. 11(1) GDPR for the sole purpose of being able to comply with the GDPR. Consequently, in some cases, no additional data should be requested in order to exercise the rights of the data subject.

However, if Mr. X tries to exercise his access right by e-mail or by regular mail, then, in this context, C will have no other choice but to ask Mr. X to provide "additional information" (Art. 12(6) GDPR) in order to be able to identify the advertising profile associated with Mr. X. In this case, the additional information will be the cookie identifier stored in the terminal equipment of Mr. X.

62. In case of demonstrated impossibility to identify the data subject (Art. 11 GDPR), the controller needs to inform the data subject accordingly, if possible, since the controller shall respond to requests from the data subject without undue delay and give reasons where it does not intend to comply with such requests. This information needs to be provided only "if possible", as the controller may not be in a position to inform the data subjects if their identification is impossible.
63. Both where the processing does not require identification and where it requires it, if the controller has reasonable doubts concerning the identity of the natural person making the request, the controller may request the provision of additional information necessary to confirm the identity of the data subject (Art.12(6) GDPR).
64. The GDPR does not impose any requirements on how to authenticate the data subject. However, Art. 11 and 12 GDPR indicate the conditions for the exercise of all the data subject rights, including the right of access to personal data.
65. It should be remembered that, as a rule, the controller cannot request more personal data than is necessary to enable this authentication, and that the use of such information should be strictly limited to fulfilling the data subjects' request.

- 66. Authentication procedures often already exist between the data subjects and the controllers. The controllers may use these authentication procedures in order to ascertain the identity of the data subjects requesting their personal data or exercising the rights granted by the GDPR<sup>30</sup>. Otherwise, controllers should implement an authentication procedure to do so<sup>31</sup>.
- 67. In cases where the controller requests or is provided by the data subject with additional information necessary to confirm the identity of the data subject, the controller shall, each time, assess what information will allow it to confirm the data subject's identity and possibly ask additional questions to the requesting person or request the data subject to present some additional identification elements, if it is proportionate (see section 3.3).
- 68. In order to allow the data subject to provide the additional information required to identify his or her data, the controller should inform the data subject of the nature of the additional information required to allow identification. Such additional information should not be more than the information initially needed for the authentication of the data subject. In general, the fact that the controller may request additional information to assess the data subject's identity cannot lead to excessive demands and to the collection of personal data which are not relevant or necessary to strengthen the link between the individual and the personal data requested<sup>32</sup>.
- 69. As a consequence, where information collected online is linked to pseudonyms or other unique identifiers, the controller can implement appropriate procedures enabling the requesting person to make a data access request and receive the data relating to them<sup>33</sup>.

**Example 12:** The data subject Ms. X requests access to her data while speaking to a helpline consultant of an electricity company with which she has concluded a contract. The consultant, having doubts as to the identity of the person making the request, generates in the company's system a one-time unique code sent to the user's mobile phone number, provided when the account was set up, as part of the double verification system, which action should be considered proportionate in this case.

### 3.3 Proportionality assessment regarding authentication of the requesting person

- 70. As indicated above, if the controller has reasonable grounds for doubting the identity of the requesting person, it may request additional information to confirm the data subject's identity. However, the controller must at the same time ensure that it does not collect more personal data than is necessary to enable authentication of the requesting person. Therefore, the controller shall carry out a proportionality assessment, which must take into account the type of personal data being processed (e.g. special categories of data or not), the nature of the request, the context within which the request is being made, as well as any damage that could result from improper disclosure. When assessing proportionality, it should be remembered to avoid excessive data collection while ensuring an adequate level of processing security.
- 71. The controller should implement an authentication procedure in order to be certain of the identity of the persons requesting access to their data<sup>34</sup>, and ensure security of the processing throughout the process of handling an access requests in accordance with Art. 32 GDPR, including for instance a secure

---

<sup>30</sup> WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 14.

<sup>31</sup> See further guidance regarding authentication in section 3.3.

<sup>32</sup> Ibid, p. 14.

<sup>33</sup> Ibid, p. 13-14.

<sup>34</sup> WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 14.

channel for the data subjects to provide additional information. The method used for authentication should be relevant, appropriate, proportionate and respect the data minimisation principle. If the controller imposes measures aimed at authentifying the data subject which are burdensome, it needs to adequately justify this and ensure compliance with all fundamental principles, including data minimisation and the obligation to facilitate the exercise of data subjects' rights (Art. 12(2) GDPR).

72. In an online context, the authentication mechanism may include the same credentials, used by the data subject to log-in to the online service offered by the controller (Recital 57 GDPR)<sup>35</sup>.
73. In practice, authentication procedures often exist and controllers do not need to introduce additional safeguards to prevent unauthorised access to services. In order to enable individuals to access the data contained in their accounts (such as an e-mail account, an account on social networks or online shops), controllers are most likely to request the logging through the login and password of the user, which in such cases should be sufficient to authenticate a data subject<sup>36</sup>. Furthermore, the data subjects are often already authenticated by the controller before entering into a contract or collecting their consent to the processing and, as a result, the personal data used to register the individual concerned by the processing can also be used as evidence to authenticate the data subject for access purposes<sup>37</sup>. Consequently, it is disproportionate to require a copy of an identity document in the event where the data subject making a request is already authenticated by the controller.
74. It should be emphasised that using a copy of an identity document as a part of the authentication process creates a risk for the security of personal data and may lead to unauthorised or unlawful processing, and, as such, it should be considered inappropriate, unless it is necessary, suitable, and in line with national law. In such cases, the controllers should have systems in place that ensure a level of security appropriate to mitigate the higher risks for the rights and freedoms of the data subject to receive such data. It is also important to note that authentication by means of an identity card does not necessarily help in the online context (e.g. with the use of pseudonyms) if the person concerned cannot contribute any other evidence, e.g. further characteristics matching to the user account.
75. Taking into account the fact, that many organisations (e.g. hotels, banks, car rentals) request copies of their clients' ID card, it should generally not be considered an appropriate way of authentication. Alternatively, the controller may implement a quick and effective security measure to identify a data subject based on the authentication it has previously carried out, e.g. via e-mail or text message containing confirmation links, security questions or confirmation codes<sup>38</sup>.
76. Information on the ID that is not necessary for confirming the identity of the data subject, such as the access and serial-number, nationality, size, eye colour, photo and machine-readable zone, depending on a case by case assessment, may be redacted or hidden by the data subject before submitting it to the controller, except where national legislation requires a full unredacted copy of the identity card (see para. 78 below). Generally, the date of issue or expiry date, the issuing authority and the full name matching with the online account are sufficient for the controller to verify the identity, always provided that the authenticity of the copy and the relation to the applicant are ensured. Additional information

---

<sup>35</sup> See further guidance regarding authentication methods in the EDPB Guidelines 01/2021 on Examples regarding Data Breach Notification, adopted on 14 January 2021, p. 30-31., and in the EDPB Guidelines 02/2021 on virtual voice assistants , Version 2.0, Adopted on 7 July 2021, section 3.7.

<sup>36</sup> WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 14.

<sup>37</sup> WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 14.

<sup>38</sup> See also Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC that has put forth different services that allow secure remote identification.

such as the birth date of the data subject may only be required in case the risk of mistaken identity persists, if the controller is able to compare it with the information it already processes.

77. To follow the principle of data minimisation the controller should inform the data subject about the information that is not needed and about the possibility to redact or hide those parts of the ID document. In such a case, if the data subject does not know how or is not able to redact such information, it is good practice for the controller to redact it upon receipt of the document, if this is possible for the controller, taking into account the means available to the controller in the given circumstances.

**Example 13:** The user Ms. Y has created a password protected account in the online store, providing her e-mail and/or username. Subsequently, the account owner asks the controller for information whether it processes their personal data, and if so, asks for access to them within the scope indicated in Art. 15. The controller requests the ID of the person making request to confirm her identity. The controller's action in this case is disproportionate and leads to unnecessary data collection.

However, in order to confirm the identity of the requesting person while preventing unnecessary data collection, the controller could require her to authenticate via logging into the account or ask her (non-intrusive) security questions, the answer to which only the data subject should know, or use multifactor authentication that were configured when the data subject registered their account, or use other existing means of communication known as to belong to the data subject, such as the e-mail address or a phone number, in order to send an access password.

**Example 14:** A bank customer, Mr. Y, plans to get a consumer credit. For this purpose, Mr. Y goes to a bank branch to obtain information, including his personal data, necessary for the assessment of his creditworthiness. To verify the data subject's identity, the consultant asks for a notarised certification of his identity to be able to provide him with the required information.

The controller should not require notarised confirmation of identity, unless it is necessary, suitable and in line with the national law (for example, where a person is temporarily not in possession of any identity document and proof of the data subject's identity is required by the national law for the performance of a legal act). Such practice exposes the requesting persons to additional costs and imposes an excessive burden on the data subjects, hampering the exercise of their right of access.

78. Without prejudice to the above general principles, under certain circumstances, authentication on the basis of an ID may be a justified and proportionate measure, in particular for entities processing special categories of personal data or undertaking data processing which may pose a risk for data subject (e.g. medical or health information). However, at the same time, it should be borne in mind that certain national provisions provide for restrictions on the processing of data contained in public documents, including documents confirming the identity of a person (also on the basis of Art. 87 GDPR). Restrictions on the processing of data from these documents may relate in particular to the scanning or photocopying of ID cards or processing of official personal identification numbers<sup>39</sup>.
79. Taking the above into account, where an ID is requested (and this is both in line with national law and justified and proportionate under the GDPR), the controller must implement safeguards to prevent unlawful processing of the ID. Notwithstanding any applicable national provisions regarding ID

<sup>39</sup> Several member states introduced such restriction in their national provisions in this regard stating, for example, that making copies of ID cards is lawful only if it results directly from the provisions of a legal act.

authentication, this may include refraining from making a copy or deleting a copy of an ID immediately after the successful authentication of the identity of the data subject. This is because further storage of a copy of an ID is likely to amount to an infringement of the principles of purpose limitation and storage limitation (Art. 5(1)(b) and (e) GDPR) and, in addition, national legislation regarding the processing of the national identification number (Art. 87 GDPR). The EDPB recommends, as good practice, that the controller, after checking the ID card, makes a note e.g. " ID card was checked " to avoid unnecessary copying or storage of copies of ID cards.

### 3.4 Requests made via third parties / proxies

80. Although the right of access is generally exercised by the data subjects as it pertains to them, it is possible for a third party to make a request on behalf of the data subject. This may apply to, among others, acting through a proxy or legal guardians on behalf of minors, as well as acting through other entities via online portals. In some circumstances, the identity of the person authorised to exercise the right of access as well as authorisation to act on behalf of the data subject may require verification, where it is suitable and proportionate (see section 3.3 above)<sup>40</sup>. It should be recalled that making personal data available to someone who is not entitled to access it can amount to a personal data breach<sup>41</sup>.
81. In doing so, national laws governing legal representation (e.g. powers of attorney), which may impose specific requirements for demonstrating authorisation to make a request on behalf of the data subject, should be taken into account, since the GDPR does not regulate this issue. In accordance with the principle of accountability, as well as of the other data protection principles, controllers shall be able to demonstrate the existence of the relevant authorisation to make a request on behalf of the data subject, and to receive the requested information, except if national law differs (e.g. national law contains specific rules regarding the trustworthiness of lawyers) leaving the controller to verify the identity of the proxy (e.g. in the case of lawyers checking enrolment at the bar). Therefore, it is recommended to collect appropriate documentation in this respect, in relation to the previously indicated general rules regarding confirmation of identity of a natural person making a request and, if the controller has reasonable doubts concerning the identity of a person acting on behalf of data subject, it shall request additional information to confirm the identity of this person.
82. While the exercise of the right of access to personal data of deceased persons amounts to another example of access by a third party other than the data subject, Recital 27 specifies that the GDPR does not apply to the personal data of deceased persons. The matter is therefore dealt with by national law and Member States may provide for rules regarding the processing of personal data of deceased persons. However, it should be borne in mind that the data may, in addition, relate to living third persons, e.g. in the context of requested access to a deceased person's correspondence. The confidentiality of such data still needs to be protected.

#### 3.4.1 Exercise of the right of access on behalf of children

83. Children deserve specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerning their rights in relation to the processing of personal

---

<sup>40</sup> Regarding the time limits for exercising the right of access when the controller needs to obtain additional information, see para. 157.

<sup>41</sup> Art. 4(12) GDPR.

data<sup>42</sup>. Any information and communication to a child, where personal data of a child are processed, should be in clear and plain language so that the child can easily understand<sup>43</sup>.

84. Children are data subjects in their own right and, as such, the right of access belongs to the child. Depending on the maturity and capacity of the child, the child may need a third party to act on its behalf e.g. the holder of parental responsibility.
85. The best interests of the child should be a leading consideration in all decisions taken with respect to the exercise of the right of access in the context of children, in particular where the right of access is exercised on behalf of the child, for example, by the holder of parental authority.
86. Due to the special protection of children's personal data contained in the GDPR, the controller shall take appropriate measures to avoid any disclosure of personal data of a minor to an unauthorised person (in this respect see also section 3.4 above).
87. Finally, the right of the holder of parental responsibility to act on behalf of the child should not be confused with instances, outside of data protection law, where national legislation may provide the right of the holder of parental responsibility to ask and receive information on the child (e.g. performance of the child at school).

### 3.4.2 Exercising the right of access through portals / channels provided by a third party

88. There are companies that provide services which enable data subjects to make access requests through a portal. The data subject signs in and gets access to a portal through which they can submit for example an access request, request data rectification or data erasure from different controllers. Different questions arise from the use of portals provided for by a third party.
89. The first issue controllers need to deal with when facing these circumstances is to ensure that the third party is acting legitimately on behalf of the data subject, as it is necessary to make sure that no data is disclosed to unauthorised parties.
90. Additionally, a controller that receives a request made through such a portal needs, invariably, to handle that request in a timely manner<sup>44</sup>. There is, however, no obligation for the controller to provide the data under Art. 15 GDPR directly to the portal, if the controller, for example, establishes that the security measures are insufficient or it would be deemed appropriate to use another way for the disclosure of data to the data subject. Under such circumstances, when the controller has other procedures in place to deal with access requests in an efficient and secure way, the controller can provide the requested information through these procedures.

---

<sup>42</sup> Recital 38 GDPR. As provided in the work programme of the EDPB, it is its intent to provide guidance on children's data. Such a document is expected to provide more guidance on the conditions under which a child may exercise their own right of access, and the holder of parental responsibility can exercise the right of access on behalf of the child.

<sup>43</sup> Recital 58 GDPR. EDPB Guidelines 05/2020 on consent under Regulation 2016/679, section 7.

<sup>44</sup> Regarding the time limits for exercising the right of access when the controller needs to obtain additional information, see para. 157

## 4 SCOPE OF THE RIGHT OF ACCESS AND THE PERSONAL DATA AND INFORMATION TO WHICH IT REFERS

91. The present section aims at shedding light on the definition of personal data (4.1) and clarifying the scope of the information covered by the right of access in general (4.2 and 4.3). Of note is that the scope of the concept of personal data and thus, the differentiation between personal data and other data, is an integral part of the assessment carried out by the controller to identify the scope of the data that the data subject is entitled to obtain access to<sup>45</sup>.
92. As a preliminary consideration it should be recalled that the right of access can only be exercised with regard to processing of personal data falling within the material and territorial scope of the GDPR. Therefore, personal data that are not processed by automated means or that are not part of or intended to become part of a filing system as per Art. 2(1) GDPR or processed by a natural person in the course of a purely personal or household activity as per Art. 2 (2) GDPR, are not covered by the right of access.

### 4.1 Definition of personal data

93. Art. 15(1) and (3) GDPR refer to “*personal data*”, and “*personal data undergoing processing*”, respectively. Therefore, the scope of the right of access is first and foremost determined by the scope of the concept of personal data, defined in Art. 4(1) GDPR<sup>46</sup>. The concept of personal data has already been the subject of several Art. 29 Working Party<sup>47</sup> documents<sup>48</sup> and has been interpreted by the CJEU, including in the context of the right of access under Art. 12 of the Directive 95/46/CE.
94. The WP29 considered that the definition of personal data in the Directive 95/46/EC “*reflects the intention of the European lawmaker for a wide notion of ‘personal data’*”<sup>49</sup>. Under the GDPR, the definition still refers to “*any information relating to an identified or identifiable natural person*”. Aside from basic personal data like name and address, telephone number etc., unlimited broad variety of data may fall within this definition, including medical findings, history of purchases, creditworthiness indicators, communication contents, etc. In light of the broad scope of the definition of personal data,

---

<sup>45</sup> In accordance with the principle of privacy by design, such analysis is part of the assessment of appropriate measures and safeguards to protect data protection principles and data subject rights, which is carried out “*at the time of the determination of the means for processing and at the time of the processing itself*”, e.g. reducing the response time when data subjects exercise their rights may be one of the metrics. For further explanations, see guidelines 4/2019 on Article 25 Data Protection by Design and by Default.

<sup>46</sup> As per Art. 4(1) GDPR, “‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;”

<sup>47</sup> The Art. 29 Working Party (Art. 29 WP) is the independent European working party that dealt with issues relating to the protection of privacy and personal data until 25 May 2018 (entry into application of the GDPR), the predecessor of the EDPB.

<sup>48</sup> e.g. WP251 rev01 Guidelines on automated individual decision-making and profiling for the purposes of regulation 2016/679 i.e., p.19; WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 9.

<sup>49</sup> WP29 Opinion 4/2007 on the concept of personal data, p. 4.

a restrictive assessment of that definition by the controller would lead to an erroneous classification of personal data<sup>50</sup> and ultimately to a violation of the right of access.

95. In joint cases C-141/12 and C-372/12<sup>51</sup> the CJEU ruled that the right of access covered personal data contained in minutes, namely the “*name, date of birth, nationality, gender, ethnicity, religion and language of the applicant*” “and, “*where relevant, the data in the legal analysis contained in the minute*”, but not the legal analysis itself<sup>52</sup>. The legal analysis was in this context not liable in itself to be the subject of a check of its accuracy by the data subject nor of rectification. Furthermore, providing access to the legal analysis does not fulfil the purpose of guaranteeing privacy but access to administrative documents.
96. In Nowak<sup>53</sup>, the CJEU made a broader analysis and found that written answers submitted by a candidate at a professional examination and any comments of an examiner with respect to those answers constitute personal data concerning the exam candidate. More precisely, such subjective information are personal data “*in the form of opinions and assessments, provided that it ‘relates’ to the data subject*”<sup>54</sup> as opposed to the examination questions, which are not considered personal data<sup>55</sup>. Thus, a contextual assessment should shed light on the effect or result an information may have on an individual and thus the scope of the right of access.

**Example 15:** An individual has a job interview with a company. In this context, the job applicant hands over a CV and an application letter. During the interview, the HR officer takes notes on a computer to document the interview. Afterwards, the job applicant, as data subject requests access to personal data relating to him or her that the company, as controller, collected in the course of the recruitment procedure.

The controller is obliged to provide the data subject with personal data actively communicated by them in their CV and letter of application. Moreover, the controller needs to provide the data subject with the summary of the interview, including the subjective comments on the behaviour of the data subject the HR officer wrote during the job interview, subject to any exemptions under national law and in compliance with Art. 23 GDPR.

97. Thus, subject to the specific facts of the case, when assessing a specific request for access, the following types of data are, *inter alia*, to be provided by controllers without prejudice to Art. 15(4) GDPR:
  - Special categories of personal data as per Art. 9 GDPR;
  - Personal data relating to criminal convictions and offences as per Art. 10 GDPR;
  - Data knowingly and actively provided by the data subject (e.g. account data submitted via forms, answers to a questionnaire)<sup>56</sup>;
  - Observed data or raw data provided by the data subject by virtue of the use of the service or the device (e.g. data processed by connected objects, transaction history, activity logs such as

---

<sup>50</sup> as information not relating to an identified or identifiable natural person.

<sup>51</sup> CJEU, joined Cases C-141/12 and C-372/12, YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S, 17 July 2014.

<sup>52</sup> CJEU, joined Cases C-141/12 and C-372/12, YS and Others, paras. 38 and 48.

<sup>53</sup> CJEU, C-434/16, Peter Nowak v Data Protection Commissioner, 20 December 2017.

<sup>54</sup> CJEU, C 434/16, Nowak, paras. 34- 35.

<sup>55</sup> CJEU, C-434/16, Nowak, para. 58.

<sup>56</sup> WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 9.

- access logs, history of website usage, search activities, location data, clicking activity, unique aspects of a person's behaviour such as handwriting, keystrokes, particular way of walking or speaking)<sup>57</sup>;
- Data derived from other data, rather than directly provided by the data subject (e.g. credit ratio, classification based on common attributes of data subjects, country of residence derived from postcode)<sup>58</sup>;
  - Data inferred from other data, rather than directly provided by the data subject (e.g. to assign a credit score or comply with anti-money laundering rules, algorithmic results, results of a health assessment or a personalization or recommendation process)<sup>59</sup>;
  - Pseudonymised data as opposed to anonymized data (see also section 3 of these guidelines).

**Example 16:** Elements that have been used to reach a decision about e.g. employee's promotion, pay rise or new job assignment (e.g. annual performance reviews, training requests, disciplinary records, ranking, career potential) are personal data relating to that employee. Thus such elements can be accessed by the data subject on request and respecting Art. 15(4) GDPR in case personal data for example, also relate to another individual (e.g. the identity or elements revealing the identity of another employee whose testimony about the professional performance is included in an annual performance review may be subject to limitations under Art. 15(4) GDPR and hence it is possible that they cannot be communicated to the data subject in order to protect the rights and freedoms of said employee). Nevertheless, national labour law provisions may apply for instance regarding the access to personnel files by employees or other national provisions such as those concerning professional secrecy. Under all circumstances, such restrictions to the exercise of the right of access of the data subject (or other rights) provided in a national law must respect the conditions of Art. 23 GDPR (see section 6.4).

98. Several considerations may be drawn from the above non-exhaustive list of personal data which may be provided to the data subject in the context of an access request. It is apparent from the above, that the controller may not operate a distinction when providing access to personal data between those data contained in paper files and those stored electronically as long as they fall within the scope of the GDPR. In other words, personal data which are contained in paper files as part of a filing system, or which are intended to form part of a filing system, are covered by the right of access in the same way as personal data stored in a computer memory by means of, for example, binary code or videotape.
99. Moreover, like most data subject rights, the right of access includes both inferred and derived data, including personal data created by a service provider, whereas the right to data portability only includes data provided by the data subject<sup>60</sup>. Therefore, in case of an access request and unlike a data portability request, the data subject should be provided not only with personal data provided to the

<sup>57</sup> WP29 Opinion 4/2007 on the concept of personal data, p. 8

<sup>58</sup> WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 10-11

<sup>59</sup> WP29 Guidelines on the right to data portability - endorsed by the EDPB, p.10-11; Art. 29 Working Party, WP 251 rev.01, 6 February 2018, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 - endorsed by the EDPB (hereinafter "WP29 Guidelines on Automated individual decision-making and profiling - endorsed by the EDPB"), p. 9-10.

<sup>60</sup> As previously stated in WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 10 and reiterated in WP29 Guidelines on Automated individual decision-making and profiling - endorsed by the EDPB, p. 17.

controller in order to make a subsequent analysis or assessment about these data but also with the result of any such subsequent analysis or assessment.

100. It also is important to recall that there is information, such as anonymous data<sup>61</sup>, which is data that do not relate directly or indirectly to an identifiable person, and that are hence excluded from the scope of the GDPR. For example, the location of the server on which the personal data of the data subject processed is not personal data. The distinction can be challenging and controllers may wonder how to draw a clear line between personal and non-personal data in particular in the case of mixed datasets. In such case it may be useful to differentiate between mixed datasets in which personal and non-personal data are inextricably linked and those in which this is not the case. Personal and non-personal data may be inextricably linked in mixed datasets and fall altogether under the scope of the right of access of the data subject to which the personal data relates<sup>62</sup>. In other cases personal and non-personal data in mixed datasets may not be inextricably linked rendering only the personal data in the set accessible to the data subject. For example, a company might need to provide a data subject with the individual IT incident reports it triggered, but not with the company's knowledge database of IT problems. However, which security measures the controller has put in place is generally not to be understood as being personal data, provided that these are not inextricably linked with personal data, and therefore not covered by the right of access.
101. Before concluding the section, the EDPB recalls in this context that the protection of natural persons with regard to the processing of personal data encompasses all the types of personal data listed above and that a restrictive interpretation of the definition contravenes the provisions of the GDPR and ultimately violates Art. 8 of the Charter of Fundamental Rights. The application of a differing regime for the exercise of a right in relation to some types of personal data, which has not been foreseen by the GDPR can be introduced exclusively by law, in accordance with Art. 23 GDPR (as further explained in section 6.4). Thus, controllers cannot limit the exercise of the right of access by unduly restricting the scope of personal data.

## 4.2 The personal data the right of access refers to

102. According to Art. 15(1) 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*"(emphasis added).
103. Several elements emerge from paragraph (1) of Art. 15 GDPR. The paragraph refers *expressis verbis* to "*personal data concerning him or her*"(4.2.1), which "*are being processed*"(4.2.2) by the controller:
  - 4.2.1 "personal data concerning him or her"
104. The right of access can be exercised exclusively with regard to personal data relating to the data subject requesting access or, where applicable, by an authorised person or proxy (see section 3.4). There are also situations in which data do not have a link to the person exercising the right of access but to

---

<sup>61</sup> Further explanations on the concept of anonymization can be found in Art. 29 Working Party, Opinion 05/2014 on Anonymisation Techniques, WP216, 10 April 2014, p. 5-19.

<sup>62</sup> Communication from the Commission to the European Parliament and the Council, Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union, 29.05.2019, COM/2019/250 final.

another individual. The data subject is however, only entitled to personal data relating to themselves excluding data which exclusively concern someone else<sup>63</sup>.

105. The classification of data as personal data concerning the data subject does, however, not depend upon the fact that those personal data also relate to someone else<sup>64</sup>. It is thus possible that personal data relate to more than one individual at the same time. This does not automatically mean that access to personal data also relating to someone else should be granted, as the controller needs to comply with Art. 15(4) GDPR.
106. The words “*personal data concerning him or her*” should not be interpreted in an “*overly restrictive*” way by controllers, as the Art. 29 Working Party already stated with regard to the right to data portability<sup>65</sup>. Applied to the right of access, the EDPB considers for example that recordings of telephone conversations (and their transcription) between the data subject that requests access and the controller, may fall under the right of access provided that the latter are personal data<sup>66</sup>. Provided that the GDPR applies and that the processing is not covered by the household exemption as per Art. 2(2)(c) GDPR, if the data subject uses the obtained record which includes personal data of the interlocutor for other purposes by, for instance, publishing the record, the data subject will become a controller for this processing of personal data relating to the other person whose voice was recorded. Although this will not exempt the controller from its data protection obligations when duly analysing whether access to the full record may be given, the controller is encouraged to inform the data subject about the fact that they may become controller in such case. This is without prejudice to any further assessment under Art. 15(4) GDPR detailed in section 6. In the same vein, messages that data subjects have sent to others in the form of interpersonal messages and deleted themselves from their device, that are still available to the service provider, may fall under the right of access.
107. Then again, there are situations in which the link between the data and several individuals may seem blurred to the controller, such as in the case of identity theft. In case of identity theft, a person fraudulently acts in the name of another person. In this context it is important to recall that the victim should be provided with information on all personal data the controller stores in connection with their identity, including those that have been collected on the basis of the fraudster’s actions. In other words, even after the controller learned about the identity theft, personal data which are associated with or related to the identity of the victim constitute personal data of the data subject.

---

<sup>63</sup> WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 9: “*Only personal data is in scope of a data portability request. Therefore, any data that is anonymous or does not concern the data subject, will not be in scope. However, pseudonymous data that can be clearly linked to a data subject (e.g. by them providing the respective identifier, cf. Article 11 (2)) is within the scope.*”

<sup>64</sup> CJEU, judgment in case C-434/16 Peter Nowak v. Data Protection Commissioner, 2017, para. 44.

<sup>65</sup> WP29 Guidelines on the right to data portability - endorsed by the EDPB, p. 9: *In many circumstances, controllers will process information that contains the personal data of several data subjects. Where this is the case, controllers should not take an overly restrictive interpretation of the sentence “personal data concerning the data subject”. As an example, telephone, interpersonal messaging or VoIP records may include (in the subscriber’s account history) details of third parties involved in incoming and outgoing calls. Although records will therefore contain personal data concerning multiple people, subscribers should be able to have these records provided to them in response to data portability requests, because the records are (also) concerning the data subject. However, where such records are then transmitted to a new controller, this new controller should not process them for any purpose which would adversely affect the rights and freedoms of the third-parties (see below: third condition)."*

<sup>66</sup> See example 34 in section 6.2.

**Example 17:** An individual fraudulently uses the identity of someone else in order to play poker online. The perpetrator pays the online casino using the credit card they stole from the victim. When the victim finds out about the identity theft, the victim asks the provider of the online casino to provide him or her with access to his or her personal data and more specifically, to the online games played and information about the credit card used by the perpetrator.

There is a link between the collected data and the victim as the latter's identity has been used. After the detection of the fraud, the personal data mentioned above still has a link by reason of their content (the victim's credit card is clearly about the victim), purpose and effect (the information about the online games played by the perpetrator may for instance be used to issue invoices to the victim). Therefore, the online casino shall grant the victim access to the aforementioned personal data.

108. If appropriate, internal connection logs can be used to hold record about accesses to a file and to trace back which actions were performed in connection with accesses to a record, such as printing, copying, or deleting personal data. These logs may include the time of logging, the reason for the access to file as well as information identifying the person having had access. Questions related to this topic are at issue in a case currently pending before the CJEU (C-579/21). The putting in place and the supervision and revision of connection logs fall within the controller's responsibility and are liable to be checked by the supervisory authorities. The controller should thus make sure that the persons acting under its authority who have access to personal data do not process personal data except on instructions from the controller, as per Art. 29 GDPR. If the person nevertheless processes the personal data for other purposes than fulfilling the controller's instructions, it may become controller for that processing and subject to disciplinary or criminal proceedings or administrative sanctions issued by supervisory authorities. The EDPB notes that it is part of the employer's responsibility under Art. 24 GDPR to make use of appropriate measures, extending from education to disciplinary procedures, to ensure that processing is in compliance with the GDPR and that no infringement occurs.

#### 4.2.2 Personal data which “are being processed”

109. Paragraph (1) of Art. 15 GDPR moreover refers to personal data, which “are being processed”. The time reference point for determining the range of personal data falling within the access request has already been elaborated in section 2.3.3. The wording however also suggests that the right of access does not distinguish between the purposes of the processing operations.

**Example 18:** A company processed personal data relating to a data subject in order to process their purchase order and arrange shipping to data subject's home address. After these initial purposes for which the personal data were collected no longer exist, the controller keeps some of the personal data solely to comply with its legal obligations relating to the keeping of records.

The data subject requests access to personal data relating to them. To comply with its obligation under article 15 (1) GDPR, the controller needs to provide the data subject with the requested personal data which are stored to comply with its legal obligations.

110. Archived personal data needs to be distinguished from back-up data that is personal data stored solely for the purpose of restoring the data in the case of a data loss event. It should be pointed out, that in respect of the principles of data protection by design and data minimisation, the back-up data is in principle similar to the data in the live system. Where there are slight differences between personal data in the back-up and the live production system, these are generally linked to the collection of additional data since the last back-up. A decrease in data in the live system (e.g. erasure after the retention period of some data came to an end or following an erasure request) will in some cases only

be overwritten in the back-up data at the time of the subsequent back-up. In case there is an access request at the moment where there are more personal data relating to the data subject in the back-up than in the live system or different personal data (noticeable for example via log of deletions in the live production system implemented in full compliance with the principle of data minimisation), the controller needs to be transparent about this situation and where technically feasible provide access as requested by the data subject, including to personal data stored in the back-up. For instance, with the aim of being transparent to data subjects who exercise their right, a log of deletions in the live production system may enable the controller to see that there are data in the back-up which are not in the live system anymore as they have been recently deleted and have not yet been overwritten in the back-up.

#### 4.2.3 The scope of a new request to access

111. What remains to say is that data subjects are entitled to have access to all data processed relating to them, or to parts of the data, depending on the scope of the request (see also 2.3.1 on the completeness of the information and 3.1.1 for the analysis of the content of the request). As a consequence, where a controller already complied with a request for access in the past and provided that the request is not excessive, the controller cannot narrow the scope of this new request. This means that in relation to any further access request of the same data subject, the controller should not inform the data subject only about the mere changes in the personal data processed or the processing itself since the last request, unless the data subject expressly agrees to this. Otherwise, data subjects would be obliged to compile their personal data provided in order to a complete set of personal data concerning their information on the processing and on data subjects rights.

### 4.3 Information on the processing and on data subject rights

112. In addition to the access to the personal data themselves, the controller has to provide information on the processing and on data subject rights according to Art. 15(1)(a) to (h) and 15(2) GDPR. Most of the information on those specific points is already compiled, at least in general form, in the controller's record of processing activities referred to in Art. 30 GDPR and/or in its privacy notice elaborated in accordance with Art.s 12 to 14 GDPR. Therefore, it might be helpful as a first step to consult the "Guidelines on transparency under Regulation 2016/679" <sup>67</sup> of the Art. 29 Working Party, on the content of the information to be given under Art. 13 and 14 GDPR.
113. In order to comply with Art. 15(1)(a) to (h) and 15(2), controllers may carefully use text modules of their privacy notice as long as they make sure that they are up-to-date and precise with regards to the request of the data subject. Before or at the beginning of the data processing, some information, such as the identification of specific recipients or the specific duration of the data processing, can often not yet be provided. Some information, like for example the right to complain to a supervisory authority (see Art. 15(1)(f)), does not change depending on the person making the access request. Therefore, it may be communicated in general terms as it is also done in the privacy notice. Other types of information, such as the information on recipients, on categories and on the source of the data may vary depending on who makes the request and what the scope of the request is. In the context of an access request under Art. 15, any information on the processing available to the controller may therefore have to be updated and tailored for the processing operations actually carried out with regard to the data subject making the request. Thus, referring to the wording of its privacy policy would

---

<sup>67</sup> Art. 29 Working Party, WP260 rev.01, 11 April 2018, Guidelines on transparency under Regulation 2016/679 - endorsed by the EDPB (hereinafter "WP29 Guidelines on transparency - endorsed by the EDPB").

not be a sufficient way for the controller to give information required by Art. 15(1)(a) to (h) and (2) unless the « tailored and updated » information is the same as the information provided at the beginning of the processing. In explaining which information relates to the requesting person, the controller could, where appropriate, refer to certain activities (such as “if you have used this service ...”, “if you have payed by invoice”) as long as it is obvious for the data subjects if they are concerned. In the following, the degree of specification required is explained in relation to the individual types of information.

114. Information on the purposes according to Art. 15(1)(a) needs to be specific as to the precise purpose(s) in the actual case of the requesting data subject. It would not be enough to list the general purposes of the controller without clarifying which purpose(s) the controller pursues in the current case of the requesting data subject. If the processing is carried out for several purposes, the controller has to clarify which data or which categories of data are processed for which purpose(s). Unlike Art. 13(1)(c) and Art. 14(1)(c) GDPR, the information on the processing referred to in Art. 15(1)(a) does not contain information on the legal basis for the processing. However, as some data subjects' rights depend on the applicable legal basis, this information is important for the data subjects to verify the lawfulness of the data processing and to determine which data subject's rights are applicable in the specific situation. Therefore, in order to facilitate the exercise of data subjects' rights in line with Art. 12(2) GDPR, the controller is recommended to also inform the data subject as to the applicable legal basis for each processing operation or to indicate where they can find this information. In any event, the principle of transparent processing requires that the information on the legal bases of the processing be made available to the data subject in an accessible way (e.g. in a privacy notice).
115. Information on categories of data (Art. 15(1)(b)) may also have to be tailored to the data subject's situation such that categories which have turned out not to be relevant in case of the requester should be eliminated.

**Example 19:** In the context of the information referred to in Art. 13/14 GDPR, a hotel states that they process a number of categories of customer data (identification data, contact data, bank data, and number of credit card etc.). If a request of access is made on the basis of Art. 15, the data subject who makes the request must, in addition to the access to the actual data being processed (component 2), in line with Art. 15(1)(b) also be informed as to the specific categories of data which are being processed in the specific case (e.g. not including bank data or credit card data in the event payment was made in cash).

116. Information on “recipients or categories of recipients” (Art. 15(1)(c)) has firstly to take into account the definition of recipients given in Art. 4(9) GDPR. The definition of recipients is based on the disclosure of personal data to a natural or legal person, public authority, agency or other body<sup>68</sup>. From Art. 4(9) GDPR follows, that public authorities acting in the framework of a particular enquiry subject to specific national provisions are not to be considered as recipients.
117. Concerning the question, if the controller is free to choose between information on recipients or on categories of recipients, it has to be noted that “unlike Art. 13 and 14 of the GDPR, which lay down an obligation on the part of the controller (...), Article 15 of the GDPR lays down a genuine right of access for the data subject, with the result that the data subject must have the option of obtaining either

---

<sup>68</sup> It should further be noted, that different controllers as defined by Art. 4(7) GDPR may exist within the same company. In this constellation a disclosure of data from one recipient to another within one company is possible.

information about the specific recipients to whom the data have been or will be disclosed, where possible, or information about the categories of recipients.”<sup>69</sup> It has also to be recalled, that, as stated in the above-mentioned guidelines on transparency<sup>70</sup>, already under Art. 13 and 14 GDPR information on the recipients or categories of recipients should be as concrete as possible in respect of the principles of transparency and fairness. Under Article 15, if the data subject has not chosen otherwise, the controller is obliged to name the actual recipients, unless it is impossible to identify those recipients or the controller demonstrates that the data subject’s requests for access are manifestly unfounded or excessive within the meaning of Article 12(5) GDPR<sup>71 72</sup>. The EDPB recalls in this regard, that storing information relating to the actual recipients is necessary *inter alia* to be able to comply with the controller’s obligations under Art. 5(2) and 19 GDPR.

**Example 20:** In its privacy notice an employer gives information about which categories of data are passed on to “travel agencies” or “hotels” in case of business trips, in accordance with Art. 13(1)(e) and 14(1)(e) GDPR. If an employee makes a request for access to the personal data after business trips have taken place, the employer should then, concerning the recipients of the personal data pursuant to Art. 15(1)(c), indicate in its reply the travel agency(ies) and hotel(s) that received the data. While the employer legitimately referred to categories of recipients in its privacy notice pursuant to Art. 13 and 14, because at this stage, it was not yet possible to name the recipients, it should, unless the employee has chosen otherwise, provide information as to the specific recipients (name of travel agencies, hotels etc.) when the employee is making an access request.

Where, respecting the conditions mentioned above, a controller may only provide the categories of recipients, the information should be as specific as possible by indicating the type of recipient (i.e. by reference to the activities it carries out), the industry, sector and sub-sector and the location of the recipients<sup>73</sup>.

118. According to Art. 15(1)(d), information has to be given on the envisaged period for which the personal data will be stored, where possible. Otherwise, the criteria used to determine that period have to be provided. The information given by the controller has to be precise enough for the data subject to know how long the data relating to the data subject will continue to be stored. If it is not possible to specify the time of deletion, the duration of storage periods and the beginning of this period or the triggering event (e.g. termination of a contract, expiration of a warranty period, etc.) shall be specified. The mere reference, for example to "deletion after expiry of the statutory storage periods" is not sufficient. Indications concerning data storage periods will have to focus on the specific data relating to the data subject. If the personal data of the data subject is subject to different deletion periods (e.g. because not all data is subject to legal storage obligations), the deletion periods shall be stated in relation to the respective processing operations and categories of data.
119. Whereas information on the right to lodge a complaint with a supervisory authority (Art. 15(1)(f)) is not dependant on the specific circumstances, the data subjects rights mentioned in Art. 15(1)(e) vary depending on the legal basis underlying the processing. With regard to its obligation to facilitate the exercise of data subject rights pursuant to Art. 12(2) GDPR, the response by the controller on those

---

<sup>69</sup> CJEU, C-154/21 (Österreichische Post AG), para. 36.

<sup>70</sup> Art. 29 Working Party, WP260 rev.01, 11 April 2018, Guidelines on transparency under Regulation 2016/679 - endorsed by the EDPB (hereinafter “WP29 Guidelines on transparency - endorsed by the EDPB”), p. 37 (Annex)

<sup>71</sup> CJEU, C-154/21 (Österreichische Post AG)

<sup>72</sup> The mere fact, that the data have been disclosed to a large number of recipients would not *per se* render the request excessive, see section 6, para 188.

<sup>73</sup> WP29 Guidelines on transparency - endorsed by the EDPB, p. 37 (Annex)

rights shall be individually tailored to the case of the data subject and relate to the processing operations concerned. Information on rights that are not applicable for the data subject in the specific situation should be avoided.

120. According to Art. 15(1)(g), “any available information” as to the source of the data has to be provided, where the personal data are not collected from the data subject. The degree of available information may change over time.

**Example 21:** The privacy policy of a large company states:

“Credit checks help us to prevent problems in payment transactions. They guarantee the protection of our company against financial risks, which can also affect sales prices in the medium to long term. A credit check is necessarily carried out when we are going to ship goods without receiving the respective purchase price at the same time, e.g. in the case of a purchase on account. Without carrying out the credit check, only a prepayment payment option (immediate bank transfer, online payment provider, credit card) is possible.

For the purpose of credit checking, we will send your name, address and date of birth to the following service providers, for example: (1) Financial Information Agency X (2) Business Information Provider Y, (3) Commercial Credit Reference Agency Z.

The data are passed on to the above-mentioned credit institutions only within the scope of what is legally permissible and only for the purposes of the analysis of your past payment behaviour as well as for the assessment of the risk of default on the basis of mathematical-statistical procedures using address data as well as for verification of your address (examination of delivery). Depending on the result of the credit check, we may no longer be able to offer you individual payment methods, such as the purchase of invoices.”

The privacy notice thus contains general information on the possibility of obtaining information from the listed Economic Information Offices in accordance with Art. 13 and 14 GDPR. If it is not clear *ex ante*, which of the companies will get involved in the processing, it is sufficient to mention the names of the eligible companies in the privacy policy. In the context of a request based on Art. 15, in addition to the information that a creditworthiness information has been obtained, it would then (*ex post*) be necessary to disclose, which of the companies mentioned has been involved exactly. It is clearly expressed by Art. 15(1)(g), that information on the processing of the data comprise “any available information as to their source” where the personal data are not collected from the data subject.

121. Art. 15(1)(h) provides that every data subject should have the right to be informed, in a meaningful way, *inter alia*, about the existence and underlying logic of automated decision-making including profiling concerning the data subject and about the significance and the envisaged consequences that such processing could have<sup>74</sup>. If possible, information under Art. 15(1)(h) has to be more specific in relation to the reasoning that lead to specific decisions concerning the data subject who asked for access.
122. Information about intended transfers of data to a third country or an international organisation, including the existence of a Commission adequacy decision or suitable safeguards, has to be given

---

<sup>74</sup> See on this behalf Guidelines on transparency under Regulation 2016/679 (WP 260), para. 41, with reference to Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (WP 251).

under Art. 13(1)(f) and 14(1)(f) GDPR. In the context of a request for access under Art. 15, Art. 15(2) requires information on the appropriate safeguards pursuant to Art. 46 GDPR only in cases where transfer to a third country or an international organisation is actually taking place.

## 5 HOW CAN A CONTROLLER PROVIDE ACCESS?

123. The GDPR is not very prescriptive as to how the controller has to provide access. The right of access may be easy and straight forward to apply in some situations, for example when a small organisation holds limited information about the data subject. In other situations, the right of access is more complicated because the data processing is more complex; with regard to the number of data subjects, the categories of processed data as well as the flow of data within and between different organisations. Considering the differences in personal data processing, the appropriate way to provide access may vary accordingly.
124. This section aims at giving some guidance and practical examples on different ways for controllers to comply with an access request as well as to the meaning of Art. 12(1) GDPR in relation to the right of access. This section will also give some guidance about what is considered to be a commonly used electronic form as well as the timing for the provision of access under Art. 12(3) GDPR.

### 5.1 How can the controller retrieve the requested data?

125. The data subjects should have access to all the information that the controller processes regarding them. This means, for example, that the controller is obliged to search for personal data throughout its IT systems and non-IT filing systems. When carrying out such search, the controller should use available information in the organisation regarding the data subject that likely will result in matches in the systems depending on how the information is structured<sup>75</sup>. For example, if the information is sorted in files depending on name or a reference number, the search could be limited to these factors. But if the structure of the data depends on other factors, such as family relations or professional titles or any kind of direct or indirect identifiers (e.g. customer number, user name or IP-addresses), the search needs to be extended to include these, provided that the controller also holds this information related to the data subject, or is provided with that information by the data subject. The same applies when records regarding third persons are likely to contain personal data regarding the data subject. The controller may, however, not require the data subject to provide more information than necessary to identify the data subject. If a controller uses a processor for its data processing activities the search naturally has to be extended to also include personal data processed by the processor.
126. In line with Art. 25 GDPR on data protection by design and by default, the controller (and any processors it uses) should also already have implemented functions enabling the compliance with data subject rights. This means, in this context, that there should be appropriate ways to find and retrieve information regarding a data subject when handling a request. However, it should be noted that an excessive interpretation in this regard could lead to functions for finding and retrieving information that in itself pose a risk for the privacy of data subjects. It is therefore important to keep in mind that the process to retrieve data should also be designed in a data protection friendly way, so that it doesn't compromise the privacy of others, for example the employees of the controller.

---

<sup>75</sup> Such a search should naturally also include information that is held by a processor, see. Article 28(3)(e) GDPR.

## 5.2 Appropriate measures for providing access

### 5.2.1 Taking “appropriate measures”

127. Art. 12 GDPR lays down the requirements for providing access, i.e. for providing the confirmation, the personal data and the supplementary information under Art. 15, and also specifies the form, manner and time limit in relation to the right of access. Art. 29 Working Party’s “Guidelines on transparency under Regulation 2016/679”<sup>76</sup> provides further guidance as regards Art. 12, mostly in relation to Art. 13 and 14 GDPR but also in relation to Art. 15 and on transparency in general. Thus, what is defined in those guidelines can often equally apply with regards to providing access under Article 15.
128. Art. 12(1) of the GDPR states that the controller shall take appropriate measures to provide any communication under Art. 15 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Art. 12(2) provides that the controller shall facilitate the data subject’s exercise of access right. The more precise requirements in this regard will have to be assessed case by case. When deciding which measures are appropriate, the controllers have to take into account all the relevant circumstances, including, but not limited to, the amount of data being processed, the complexity of their data processing and the knowledge they have about their data subjects, for example if the majority of the data subjects are children, elderly people or people with disabilities. In addition, in situations where the controller is made aware of any particular needs of the data subject making the request, for example through additional information in the request made, the controller needs to take these circumstances into consideration. As a result the appropriate measures will vary.
129. It is important to keep in mind when making the assessment that the term “appropriate” should never be understood as a way of limiting the scope of the data covered by the right of access. The term “appropriate” does not mean that the efforts to provide the information can be balanced against, for example, any interest the data subject may have in obtaining the personal data. Instead the assessment should aim at choosing the most appropriate method for providing all information covered by this right, depending on the specific circumstances in each case. As a consequence, a controller who processes a large quantity of data on a large scale must accept to undertake great efforts to ensure the right of access to the data subjects in a concise, transparent, intelligible and easily accessible form, by using plain and clear language.
130. It needs to be avoided to direct the data subject to different sources in response to a data access request. As previously stated in the WP29 Guidelines on Transparency (with regard to the notion of “provide” in Art. 13 and 14 GDPR), the notion of “provide” entails that *“the data subject must not have to actively search for information covered by these articles amongst other information, such as terms and conditions of use of a website or app”*<sup>77</sup>. Therefore, and in respect of the transparency principle, data subjects must obtain from the controller the information and personal data required by Art. 15(1), 15(2) and 15(3) in a way that enables complete access to the requested information. In special circumstances, it would be inappropriate or even unlawful to share the information within the controller, for example due to the sensitive nature of the information (such as information relating to whistleblowing). In these cases, it would be deemed appropriate to split the information into several replies as a response to the data subjects access request. The method chosen by the controller must

---

<sup>76</sup> Art. 29 Working Party, WP260 rev.01, 11 April 2018, Guidelines on transparency under Regulation 2016/679 - endorsed by the EDPB (hereinafter “WP29 Guidelines on transparency - endorsed by the EDPB”).

<sup>77</sup> WP29 Guidelines on transparency - endorsed by the EDPB, para. 33.

actually provide the data subject with the requested data and information, hence it would not be appropriate to solely refer the data subject to check the requested data stored on their own device including, for example, to check clickstream history and IP addresses on their mobile phone.

131. In accordance with the accountability principle, a controller must document their approach to be able to demonstrate how the means chosen to provide the necessary information under Art. 15 are appropriate in the circumstances at hand.

## 5.2.2 Different means to provide access

132. As already explained in section 2.2.2 above, when making an access request the data subjects are entitled to receive a copy of their data undergoing processing pursuant to Art. 15(3) together with the supplementary information, which is considered as the main modality for providing access to the personal data.
133. However, in some circumstances it could be appropriate for the controller to provide access through other ways than providing a copy. Such non-permanent modalities of access to the data could be, for example: oral information, inspection of files, onsite or remote access without possibility to download. These modalities may be appropriate ways of granting access for example in cases where it is in the interest of the data subject or the data subject asks for it. Onsite access could also be appropriate, as an initial measure, when a controller handles a large quantity of non-digitalized data to allow the data subject to be made aware of what personal data are undergoing processing and to be able to make an informed decision about what personal data he or she wants to be provided through a copy. Non-permanent ways of access can be sufficient and adequate in certain situations; for example, it can satisfy the need of the data subjects to verify that the data processed by the controller are correct by giving data subjects a chance to view the original data. A controller is not obliged to provide the information through other ways than providing a copy but should take a reasonable approach when considering such a request. Giving access through other ways than providing a copy does not preclude the data subjects from the right to also have a copy, unless they choose not to.
134. The controller may choose, depending on the situation at hand, to provide the copy of the data undergoing processing, together with the supplementary information, in different ways, e.g. by e-mail, physical mail or by the use of a self-service tool. If the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form as stated in Art. 15(3). In any case, the controller has to consider appropriate technical and organizational measures, including adequate encryption when providing information via e-mail or online-self-service tools.
135. In the situation, where the controller is processing personal data regarding the person making the request only in a small scale, the copy of the personal data and the supplementary information can and should be provided through a simple procedure.

**Example 22:** A local bookstore keeps a record of name and addresses of their customers that have ordered home delivery. A customer visits the bookstore and makes a request for access. In this situation it would be sufficient to print out the personal data concerning the customer directly from the business system, while also supplying the supplementary information in Art. 15(1) and (2).

**Example 23:** A monthly donor to a charity organisation makes an access request through e-mail. The charity organisation holds information about donations made in the past twelve months, as well as names and e-mail addresses of the donors. The controller could provide the copy of the personal data

and the supplementary information by responding to the e-mail, provided that all necessary safeguards are applied, taking into consideration for example the nature of the data.

136. Even controllers that process a large quantity of data can choose to rely on manual routines for handling access requests. If the controller processes data in several different departments, the controller needs to collect the personal data from each department to be able to respond to the data subject request.

**Example 24:** An administrator is appointed by the controller to handle the practical issues regarding access requests. When receiving a request the administrator sends an enquiry by e-mail to the different departments of the organisation asking them to collect personal data regarding the data subject. Representatives of each department give the administrator the personal data processed by their department. The administrator then sends all the personal data to the data subject together with the necessary supplementary information, for example and when appropriate, by e-mail.

137. Although manual processes for handling access requests could be regarded as appropriate, some controllers may benefit from using automated processes to handle data subject requests. This could, for example, be the case for controllers that receive a large number of requests. One way to provide the information under Art. 15 is by providing the data subject with self-service tools. This could facilitate an efficient and timely handling of data subjects' requests of access and will also enable the controller to include the verification mechanism in the self-service tool.

**Example 25:** A social media service has an automated process for handling access requests in place that enables the data subject to access their personal data from their user account. To retrieve the personal data the social media users can choose the option to "Download your personal data" when logged into their user account. This self-service option allows the users to download a file containing their personal data directly from the user account to their own computer.

138. The use of self-service tools should never limit the scope of personal data received. If not possible to give all the information under Art. 15 through the self-service tool, the remaining information needs to be provided in a different manner. The controller may indeed encourage the data subject to use a self-service tool that the controller has set in place for handling access requests. However, it should be noted that the controller must also handle access requests that are not sent through the established channel of communication<sup>78</sup>.

### 5.2.3 Providing access in a "concise, transparent, intelligible and easily accessible form using clear and plain language"

139. According to Art. 12(1) GDPR the controller shall take appropriate measures to provide access under Art. 15 in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
140. The requirement that providing access to the data subject has to be done in a concise and transparent form means, that controllers should present the information efficiently and succinctly in order to be easily understood by the data subject, especially if it is a child. The controller needs to take into account the quantity and complexity of the data when choosing the means for providing access under Art. 15.

**Example 26:** A social media provider processes a large quantity of information about a data subject. A large part of this personal data is information contained in hundreds of pages of log files where the

---

<sup>78</sup> See section 3.1.2.

data subject's activities on the website are registered. If data subjects request access to their personal data, the personal data in these log files are indeed covered by the right of access. The right of access may therefore be formally fulfilled if these hundreds of pages of log files were to be provided to the data subject. However, without measures taken to facilitate the understanding of the information in the log files, the data subject's right of access might not be met in practice, because no knowledge can easily be drawn from the log files, therefore not fulfilling the requirement of Art. 12(1) GDPR. The controller must therefore be careful and thorough when choosing the way the information and personal data is presented to the data subject.

141. Under the circumstances in the example above, the use of a layered approach, similar to the layered approach advocated in the Guidelines on transparency with regard to privacy notices<sup>79</sup>, could be an appropriate measure to fulfil both the requirements in Art. 15 and 12(1) GDPR. This will be further developed under section 5.2.4. below. The requirement that the information is "intelligible" means that it should be understood by the intended audience<sup>80</sup>, whilst keeping in mind any particular needs that the data subject might have that is known to the controller<sup>81</sup>. Since the right of access often enables the exercise of other data subject rights, it is crucial that the information provided is made understandable and clear. This is because data subjects will only be able to consider whether to invoke their right to, for example, rectification under Art. 16 GDPR once they know what personal data are being processed, for what purposes etc. As a result, the controller might need to supply the data subject with additional information that explains the data provided. It should be emphasised that the complexity of data processing obliges the controller to provide the means to make the data understandable and could not be used as an argument to limit the access to all data. Similarly, the controller's obligation to provide data in a concise manner cannot be used as an argument to limit access to all data.

**Example 27:** An ecommerce website collects data about items viewed or purchased on its website for marketing purposes. A part of this data will consist of data in a raw format<sup>82</sup>, which has not been analysed and may not be directly meaningful to the reader (codes, activity history etc.). Such data related to the data subjects activities is also covered by the right of access and should, as a consequence, be provided to the data subject in response to an access request. When providing data in a raw format it is important that the controller takes the necessary measures to ensure that the data subject understands the data, for example, by providing an explanatory document that translates the raw format into a user friendly form. Also, such a document could explain that abbreviations and other acronyms for example "A" means that the purchase has been interrupted and "B" means that the purchase has gone through.

142. The "easily accessible" element means that the information under Art. 15 should be presented in a way that is easy for the data subject to access. This applies for example, to the layout, appropriate

---

<sup>79</sup> WP29 Guidelines on transparency - endorsed by the EDPB, para. 35.

<sup>80</sup> Intelligibility is closely linked to the requirement to use a plain and clear language (WP29 Guidelines on transparency - endorsed by the EDPB, para. 9). What is said about a plain and clear language in para. 12-16 with regards to information referred to in Articles 13 and 14 GDPR, equally applies to communication under Article 15.

<sup>81</sup> See para. 128.

<sup>82</sup> The raw format in the example is to be understood as unanalysed data underlying a processing, and not the lowest level of raw data that may only be machine-readable (such as "bits").

headings and paragraphing. The information should always be provided in plain and clear language. A controller that offers a service in a country should also offer answers in the language that is understood by the data subjects in that country. The use of standardised icons is also encouraged when it facilitates the intelligibility and accessibility of the information. When the request for information relates to visually impaired data subjects or other data subjects who may have difficulty in accessing or understanding information, the controller is expected to take measures facilitating the understanding of the information provided, including oral information, when adequate<sup>83</sup>. The controller should take special care to ensure that elderly people, children, visually impaired persons or persons with cognitive or other disabilities can exercise their rights, for instance, by proactively providing easily accessible elements to facilitate exercise of these rights.

#### 5.2.4 A large quantity of information necessitates specific requirements on how the information is provided

143. Regardless of the means used to provide access there may be a tension between the amount of information the controller needs to provide data subjects with and the requirement that it must be concise. One way of achieving both, and an example of an appropriate measure for certain controllers, when a large quantity of data is to be provided, is to use a layered approach. This approach can facilitate the data subjects' understanding of the data. It should nevertheless be stressed that this approach can only be used under certain circumstances and needs to be carried out in a way that does not limit the right of access, as explained below. Furthermore, the use of a layered approach should not create an extra burden for the data subject. Hence, it would be best suited when access is provided in an online context. A layered approach is merely a way to present the information under Art. 15 in a manner which is also compliant with the requirements in Art. 12(1) GDPR and should not be confused with the possibility for the controllers to request that the data subject specifies the information or processing activities to which the request relates, as prescribed in Recital 63 of the GDPR<sup>84</sup>.
144. A layered approach in relation to the right of access means that a controller, under certain circumstances, can provide the personal data and the supplementary information required under Art. 15 in different layers. The first layer should include information about the processing and data subject's rights according to Art. 15(1)(a)-(h) and 15(2) as well as a first part of the processed personal data. In a second layer, more personal data should be provided.
145. When deciding what information should be given in the different layers the controller should consider what information the data subject in general would consider as most relevant. In line with the fairness principle, the first layer should also contain information on the processing which has the most impact on the data subject<sup>85</sup>. The controllers need to be able to demonstrate accountability as to their reasoning of the above.

**Example 28:** A controller analyses big data sets to place customers in different segments depending on their online behaviour. In this situation, it can be assumed that the information that is the most important for the data subjects to obtain is information about what segment they have been put in. As a result, this information should be included in the first layer. The data in a raw format<sup>86</sup> that has not yet been analysed or further processed, such as user activity on a website, is also personal data

---

<sup>83</sup> See WP29 Guidelines on transparency - endorsed by the EDPB, para. 21.

<sup>84</sup> See also section 2.3.1.

<sup>85</sup> See WP29 Guidelines on transparency - endorsed by the EDPB, para. 36.

<sup>86</sup> See footnote 82.

covered by the right of access, however, it could in some cases be sufficient to provide this information in another layer.

146. For the use of layered approach to be considered as an appropriate measure, it is necessary that the data subject is informed at the outset that the information under Art. 15 is structured into different layers and provided with a description of what personal data and information that will be contained in the different layers. In this way it will be easier for the data subject to decide what layers they want to access. The description should objectively reflect all the categories of personal data that are actually processed by the controller. It also needs to be clear how the data subject can get access to the different layers. Access to the different layers shall not entail any disproportionate effort for the data subject and shall not be made conditional on the formulation of a new data subject request. This means that the data subjects must have the possibility to choose whether to access all layers at once or to access one or two of the layers, if they are satisfied with this.

**Example 29:** A data subject makes an access request to a video streaming service. The request is made through an option that is available when data subjects have logged into their account. The data subject is presented with two options which appear as buttons on the webpage. Option one is to download part 1 of the personal data and the supplementary information. This contains, for example, recent streaming history, account information and payment information. Option two is to download part 2 of the personal data that contains technical log files about the data subjects activities and historical information on the account. In this case, the controller has made it possible for data subjects to exercise their right in a way that does not create an extra burden for the data subject.

**Variation 1:** In cases where the data subject only chooses the button to download part 1 of the personal data, the controller is obliged only to provide part 1 of the data.

**Variation 2:** In cases where the data subject chooses the buttons for both part 1 and part 2 of the data, the controller cannot communicate only part 1 of the data and ask for a new confirmation before communication of part 2 of the data. Instead both parts of the data must be provided to the data subject, as it follows from the request made.

147. The use of a layered approach will not be considered appropriate for all controllers or in all situations. It should only be used when it would be difficult for the data subject to comprehend the information if given in its entirety. In other words, the controller needs to be able to demonstrate that the use of layered approach adds value for the data subject in helping them understand the information provided. A layered approach would therefore only be considered appropriate when a controller processes a large quantity of personal data about the data subject making a request and where there would be apparent difficulties for the data subject to grasp or comprehend the information if it were to be provided all at once. The fact that it would require great effort and resources from the controller to provide the information under Art. 15 is not in itself an argument for using a layered approach.

## 5.2.5 Format

148. According to Art. 12(1) GDPR, information under Art. 15 shall be provided in writing or by other means including, where appropriate, by electronic means. As regards access to the personal data undergoing processing, Art. 15(3) states that where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form. The GDPR does not specify what a commonly used electronic form is. Thus there are several conceivable formats that can be used. What is considered to be a commonly used electronic form will also vary over time.

149. What could be considered as a commonly used electronic form should be based on an objective assessment and not on what format the controller uses in its daily operations. In order to determine what format is to be considered as a commonly used format in the situation at hand, the controller will have to assess if there are specific formats generally used in the controller's area of operation or in the given context. When there are no such formats generally used, open formats set in an international standard, such as ISO, should, in general, be considered as commonly used electronic formats. However, the EDPB does not exclude the possibility that other formats may also be considered to be commonly used within the meaning of Article 15(3). When assessing if a format is a commonly used electronic format, the EDPB considers that it is of importance how easily the individual can access information provided in the current format. In this regard it should be noted what information the controller has provided to the data subject about how to access a file which has been provided in a specific format, such as what programs or software that could be used, to make the format more accessible to the data subject. The data subject should, however, not be obliged to buy software in order to get access to the information.
150. When deciding upon the format in which the copy of the personal data and the information under Art. 15 should be provided, the controller needs to keep in mind that the format must enable the information to be presented in a way that is both intelligible and easily accessible. It is important that the data subject is provided with information in embodied, permanent form (text, electronic). Since the information should persist over time, information in writing, including by electronic means, is, in principle, preferable over other forms. The copy of the personal data could, when appropriate, be stored on an electronic storage device such as CD or USB.
151. It should be noted that for a controller to be able to consider that data subjects have been provided with a copy of personal data it is not enough to have provided them with access to their personal data. For the requirement to provide a copy of personal data to be fulfilled and in case the data are provided electronically/digitally, the data subjects need to be able to download their data in a commonly used electronic form.
152. It is the responsibility of the controller to decide upon the appropriate form in which the personal data will be provided. The controller can, although is not necessarily obliged to, provide the documents which contain personal data about the data subjects making the request, in their original form. The controller could, for example, on a case-by-case basis, provide access to a copy of the medium as such, given the need for transparency (for example, to verify the accuracy of the data held by the controller in the event of a request for access to the medical file or an audio recording whose transcript is disputed). However, the CJEU, in its interpretation of the right of access under the Directive 95/46/EC, stated that "for [the right of access] to be complied with, it is sufficient for the applicant to be provided with a full summary of those data in an intelligible form, that is, a form which allows him to become aware of those data and to check that they are accurate and processed in compliance with that directive, so that he may, where relevant, exercise the rights conferred on him"<sup>87</sup>. Unlike the directive, the GDPR expressly contains an obligation to provide the data subject with a copy of the personal data undergoing processing. This, however, does not mean that the data subject always has the right to obtain a copy of the documents containing the personal data, but an unaltered copy of the personal data being processed in these documents.<sup>88</sup> Such copy of the personal data could be provided through a compilation containing all personal data covered by the right of access as long as the compilation

---

<sup>87</sup> CJEU, Joined Cases C-141/12 and 372/12, YS and Others, para. 60.

<sup>88</sup> Questions related to this topic are at issue in cases currently pending before the CJEU ( C-487/21 and C-307/21).

makes it possible for the data subject to be made aware and verify the lawfulness of the processing. Hence, there is no contradiction between the wording of the GDPR and the ruling by the CJEU regarding this matter. The word summary in the ruling should not be misinterpreted as meaning that the compilation would not encompass all data covered by the right of access, but is merely a way to present all that data without giving access to the underlying documents which contain the personal data. Since the compilation needs to contain a copy of the personal data, it should be stressed that it cannot be made in a way that somehow alters or changes the content of the information.

**Example 30:** A data subject has been insured with an insurance company for many years. Several insured incidents have occurred. In each case there has been some written correspondence through e-mail between the data subject and the insurance company. As the data subject had to provide information regarding the specific circumstances of each incident, the correspondence entails a lot of personal information about the data subject (hobbies, flatmates, daily habits etc.). In some cases disagreement arose about the insurance company's obligation to compensate the data subject which caused a vast amount of communication back and forth. All this correspondence is stored by the insurance company. The data subject makes an access request. In this situation the controller does not necessarily have to provide the e-mails in their original form by forwarding them to the data subject. Instead the controller could choose to compile the e-mail correspondence containing the data subject's personal data in a file that is provided to the data subject.

153. Notwithstanding the form in which the controller provides the personal data, e.g. by providing the actual documents containing the personal data or a compilation of the personal data, the information shall comply with the transparency requirements laid down in Art. 12 GDPR. Making some kind of compilation and/or extracting the data in a way that makes the information easy to comprehend could, in some cases, be a way to comply with these requirements. In other cases the information is better understood by providing a copy of the actual document containing the personal data. Hence which form is most suitable must be decided on a case by case basis.
154. In this context, it is important to remember that there is a distinction between the right to obtain access under Art. 15 GDPR and the right to receive a copy of administrative documents regulated under national law, the latter being a right to receive a copy of the actual document. This does not mean that the right of access under Art. 15 GDPR excludes the possibility to receive a copy of the document/media on which the personal data appear.
155. In some cases, the personal data itself sets the requirements in what format the personal data should be provided. For example, when the personal data constitutes handwritten information by the data subject, the data subject may need to be provided with a photocopy of that handwritten information, as the handwriting itself is personal data. That could especially be the case when the handwriting is something that matters to the processing, e.g. scripture analysis. The same applies in general for audio recordings because the voice of the data subject itself is personal data. In some cases, however, access can be given by providing a transcription of the conversation, for example, if agreed upon between the data subject and the controller.
156. It should be noted that the provisions on format requirements are different regarding the right of access and the right of data portability. Whilst the right of data portability under Art. 20 GDPR requires that the information is provided in a machine readable format, the right to information under Art. 15 does not. Hence, formats that are considered not to be appropriate when complying with a data portability request, for example pdf-files, could still be suitable when complying with an access request.

### 5.3 Timing for the provision of access

157. Art. 12(3) GDPR requires that the controller provides information to the data subject regarding action taken in respect of a request under Art. 15 without undue delay and in any event within one month of receipt of the request. This deadline can be extended by a maximum of two months taking into account the complexity and the number of the requests, provided that the data subject has been informed about the reasons for such delay within one month of the receipt of the request. This obligation to inform the data subject about the extension and its reasons should not be confused with the information that has to be given without delay and at the latest within one month when the controller does not take action on the request, as detailed by Art. 12(4) GDPR.
158. The controller shall react and, as a general rule, provide the information under Art. 15 without undue delay, which means that the information should be given as soon as possible. This means that, if it is possible to provide the requested information in a shorter amount of time than one month, the controller should do so. The EDPB also considers that the timing to answer the request in some situations must be adapted to the storage period in order to be able to provide access<sup>89</sup>.
159. The time limit starts when the controller has received an Art. 15 request, meaning when the request reaches the controller through one of its official channels.<sup>90</sup> It is not necessary that the controller is in fact aware of the request. However, when the controller needs to communicate with the data subject due to the uncertainty regarding the identity of the person making the request there may be a suspension in time until the controller has obtained the information needed from the data subject, provided the controller has asked for additional information without undue delay. The same applies for when a controller has asked a data subject to specify the processing operations to which the request relates, when the conditions set out in Recital 63 are met.<sup>91</sup>

**Example 31:** Following the reception of the request, a controller reacts immediately and asks the information it needs to confirm the identity of the person making the request. The latter replies only several days later and the information that the data subject sends to verify the identity does not seem sufficient which requires the controller to ask for clarifications. In this situation there will be a suspension in time until the controller has obtained enough information to verify the identity of the data subject.

160. The time period to respond to an access request needs to be calculated in accordance with Regulation No 1182/71<sup>92</sup>.

**Example 32:** An organisation receives a request on 5 March. The time limit starts from the same day. This gives the organisation until and including 5 April to comply with the request, at the latest.

---

<sup>89</sup> See section 2.3.3

<sup>90</sup> In some member states there is national law determining when a message is to be considered as received, taking into account weekends and national holidays.

<sup>91</sup> See further section 2.3.1.

<sup>92</sup> Regulation (EEC, EURATOM) No 1182/71 of the Council of 3 June 1971 determining the rules applicable to periods, dates and time limits.

**Example 33:** If the organisation receives a request on 31 August, and as the following month is shorter there is no corresponding date, the date for response, at the latest, is the last day of the following month, hence 30 September.

161. If the last day of this time period falls on a weekend or a public holiday, the controller has until the next working day to respond.
162. Under certain circumstances the controller can extend the time to respond to a request of access by two further months if necessary, taking into account the complexity and number of the requests. It should be emphasised that this possibility is an exemption from the general rule and should not be overused. If controllers often find themselves forced to extend the time limit, it could be an indication of a need to further develop their general procedures to handle requests.
163. What constitutes a complex request varies depending upon the specific circumstances of each case. Some of the factors that could be considered relevant are for example:
  - the amount of data processed by the controller,
  - how the information is stored, especially when it is difficult to retrieve the information, for example when data are processed by different units of the organisation,
  - the need to redact information when an exemption applies, for example information regarding other data subjects or that constitutes trade secrets, and
  - when the information requires further work in order to be intelligible.
164. The mere fact that complying with the request would require a large effort does not make a request complex. Similarly, the fact that a big company receives a large number of requests would not automatically trigger an extension of the time limit. However, when a controller temporarily receives a large amount of requests, for example due to an extraordinary publicity regarding their activities, this could be regarded as a legitimate reason for prolonging the time of the response. Nevertheless, a controller, especially one who handles a large quantity of data, should have procedures and mechanisms in place in order to be able to handle requests within the time limit under normal circumstances.

## 6 LIMITS AND RESTRICTIONS OF THE RIGHT OF ACCESS

### 6.1 General remarks

165. The right of access is subject to the limits that result from Art. 15(4) GDPR (rights and freedoms of others) and Art. 12 (5) GDPR (manifestly unfounded or excessive requests). Furthermore, Union or Member State law may restrict the right of access in accordance with Art. 23 GDPR. Derogations regarding the processing of personal data for scientific, historical research or statistical purposes or archiving purposes in the public interest can be based on Art. 89(2) and Art. 89(3) GDPR accordingly and derogations for processing carried out for journalistic purposes or the purpose of academic, artistic or literary expression can be based on Art. 85(2) GDPR.
166. It is important to note that, apart from the above mentioned limits, derogations and possible restrictions, the GDPR does not allow any further exemptions or derogations to the right of access. That means *inter alia* that the right of access is without any general reservation to proportionality with regard to the efforts the controller has to take to comply with the data subjects request under Art. 15

GDPR<sup>93</sup>. Furthermore, it is not permitted to limit or restrict the right of access in a contract between the controller and the data subject.

167. According to Recital 63, the right of access is granted to data subjects in order to be aware of, and verify, the lawfulness of the processing. The right of access enables, *inter alia*, the data subject to obtain, depending on the circumstances, the rectification, erasure or blocking of personal data<sup>94</sup>. However, data subjects are not obliged to give reasons or to justify their request. As long as the requirements of Art. 15 GDPR are met the purposes behind the request should be regarded as irrelevant<sup>95</sup>.

## 6.2 Article 15 (4) GDPR

168. According to Art. 15(4) GDPR, the right to obtain a copy shall not adversely affect the rights and freedoms of others. Explanations about this limitation are given in the fifth and sixth sentences of Recital 63. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject. When interpreting Art. 15(4) GDPR special caution has to be taken not to unjustifiably widen the restrictions laid down in Art. 23 GDPR, which are permissible only under strict conditions.
169. Art. 15(4) GDPR applies to the right to obtain a copy of the data, which is the main modality of giving access to the data processed (second component of the right of access). It is also applicable, and rights and freedoms of others shall be taken into account, if access to the personal data is exceptionally granted by other means than a copy. For example, there is no difference justified whether trade secrets are affected by providing a copy or by granting on site access to the data subject. Art. 15(4) GDPR is not applicable to the additional information on the processing as stated in Art. 15(1) lit. a.-h. GDPR.
170. According to Recital 63, conflicting rights and freedoms include trade secrets or intellectual property and in particular the copyright protecting the software. These explicitly mentioned rights and freedoms should be regarded merely as examples, as, in principle, any right or freedom based on Union or Member State law may be considered to invoke the limitation of Art. 15(4) GDPR<sup>96</sup>. Thus, the right to the protection of personal data (Art. 8 European Charter of Fundamental Rights) can also be considered as an affected right in terms of Art. 15(4) GDPR. Regarding the right to obtain a copy, the right to data protection of others is a typical case where the limitation needs to be assessed. Furthermore, the right to confidentiality of correspondence has to be taken into account, for example with regard to private e-mail-correspondence in the employment context<sup>97</sup>. It is important to note that not every interest amounts to “rights and freedoms” pursuant to Art. 15(4) GDPR. For example, the economic interests of a company not to disclose personal data do not reach the threshold for the

---

<sup>93</sup> Where the controller processes a large quantity of information concerning the data subject, as mentioned in recital 63 GDPR, the controller may request the data subject to specify the information or processing activities to which the request relates. See also section 2.3.1.

<sup>94</sup> CJEU, Joined Cases C-141/12 and C-372/12, YS and Others.

<sup>95</sup> This is without prejudice to any applicable national law that comply with the requirements posed by Art. 23 GDPR, see Chapter 6.4.

<sup>96</sup> The weight or priority of the conflicting rights and freedoms is not a question of the definition of the terms “rights and freedoms”. However, balancing of such interests is part of a second step of the assessment, whether Art. 15(4) is applicable. See para. 173 below.

<sup>97</sup> ECHR, Bărbulescu v. Romania, no 61496/08, para. 80, 5 September 2017.

recourse to the exemption in Art. 15(4) as long as there are no trade secrets, intellectual property or other protected rights affected.

171. “Others” means any other person or entity apart from the data subject who is exercising their right of access. Hence, the rights and freedoms of the controller or processor (in keeping trade secrets and intellectual property confidential for example) might be considered. If the EU legislator wanted to exclude controllers or processors rights and freedoms, it would have used the term “third party”, which is defined in Art. 4(10) GDPR.
172. The general concern that rights and freedoms of others might be affected by complying with the request for access, is not enough to rely on Art. 15 (4) GDPR. The controller must be able to demonstrate that in the concrete situation, rights or freedoms of others would, in fact, be impacted.

**Example 34:** A person who is now an adult was cared for by the youth welfare office over a number of years in the past. The corresponding files may possibly contain sensitive information about other persons (parents, social workers, other minors). However, a request for information from the data subject cannot generally be rejected for this reason with reference to Art. 15(4) GDPR. Rather, the rights and freedoms of others must be examined in detail and demonstrated by the youth welfare office as the controller. Depending on the interests in question and their relative weight, providing such specific information may be rejected (e.g. by redacting names).

173. With regard to Recital 4 GDPR and the rationale behind Art. 52(1) of the European Charter of Fundamental Rights, the right to protection of personal data is not an absolute right<sup>98</sup>. Hence also the exercise of the right of access has to be balanced against other fundamental rights in accordance with the principle of proportionality. When the Art. 15(4) GDPR assessment proves that complying with the request has adverse (negative) effects on other participants’ rights and freedoms (step 1), the interests of all participants need to be weighed taking into account the specific circumstances of the case and in particular the likelihood and severity of the risks present in the communication of the data. The controller should try to reconcile the conflicting rights (step 2), for example through the implementation of appropriate measures mitigating the risk to the rights and freedoms of others. As emphasised in Recital 63, protecting the rights and freedoms of others by virtue of Art. 15(4) GDPR should not result in a refusal to provide all information to the data subject. This means, for example, where the limitation applies, that information concerning others has to be rendered illegible as far as possible instead of refusing to provide a copy of the personal data. However, if it is impossible to find a solution of reconciliation of the relevant rights, the controller has to decide in a next step which of the conflicting rights and freedoms prevails (step 3).

**Example 35:** A retailer offers its clients the possibility to order products via a hotline operated by its customer service. For the purpose of proving the commercial transactions, the retailer stores a call recording, in accordance with the strict requirements of applicable legislation. A customer wants to receive a copy of the conversation he had with an agent of the customer service. In a first step, the retailer analyses the request and realises that the record contains personal data that also relate to someone else, namely to the agent of the customer service. In a second step, in order to assess whether providing the copy would affect the rights and freedoms of others, the retailer has to balance the conflicting interests, especially taking into account the likelihood and severity of possible risks to the rights and freedoms of the customer service agent, that are present in the communication of the record to the client. The retailer concludes that there are very limited

<sup>98</sup> See, for example, also CJEU, Joined cases C-92/09 and C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen [GC], 9 November 2010, para. 48.

personal data relating to the customer service agent in the record, only his voice. The retailer/controller finds that the agent is not easily identifiable. Moreover, the content of the discussion is of a professional nature and the data subject was the interlocutor. On the basis of the aforementioned circumstances the controller objectively concludes that the right to access does not adversely affect the rights and freedoms of the agent of the customer service and therefore, the controller may provide the data subject with the full record, including the parts of the voice record that relate to the agent of the customer service.

**Example 36:** A client of a medical supply store wants access to the measuring results concerning her legs on the basis of Art. 15 GDPR. The medical supply store had measured the data subject's legs in order to craft individual medical compression stockings. Apparently the medical supply store had a lot of experience and had established a special technique to measure accurately. After the measuring in the medical supply store, the client wants to use the measuring results to buy cheaper socks elsewhere (ordering them in an online-shop). The medical supply store partially refuses access to the data on the basis of Art. 15(4) GDPR claiming that due to their special, accurate measuring techniques the results were protected as trade secrets. If and in so far the controller is able to prove that:

- providing the data subject with information about the measuring results is not possible without revealing how the measurements were taken and
- the information about how the measurements were taken including, if relevant, the exact determination of the measuring points are trade secrets

they may apply Art. 15(4) GDPR.

The controller would still have to provide as much information as it could about the measuring results that would not reveal its trade secret, even if that would imply the effort to revise and edit the results.

**Example 37:** GAMER X is registered as a user on the gaming platform of PLATFORM Y. One day, GAMER X is notified that his online account has been restricted. As he is unable to log in anymore, GAMER X asks the controller for access to all personal data relating to him. In addition, GAMER X requires access to the reasons for the account restriction. PLATFORM Y, the controller of the online gaming platform with which the request has been lodged, informs the users in its general terms and conditions available on its website, that any kind of cheating (mainly by the use of third party software) will entail a temporal or permanent ban from its platform. PLATFORM Y also informs the users in its privacy policy about the processing of personal data for the purpose of detecting gaming cheats, in accordance with the requirements set out in Art. 13 GDPR.

Upon receipt of GAMER X's request for access, PLATFORM Y should provide GAMER X with a copy of the personal data processed about GAMER X. Regarding the reason for the account restriction, PLATFORM Y should confirm GAMER X that it decided to restrict GAMER X's access to online games due to the use of one or repeated gaming cheats which are in violation with the general terms of use. In addition to the information provided about the processing for the purpose of gaming cheat detection, PLATFORM Y should grant GAMER X access to the information it has stored about GAMER X's gaming cheats which led to the restriction. In particular, PLATFORM Y should provide GAMER X with the information that led to the restriction of the account (e.g. log overview, date and time of

cheating, detection of third party software,...) in order for the data subject (*i.e.* GAMER X) to verify that the data processing has been accurate.

However, according to Art. 15(4) GDPR and Recital 63 GDPR, PLATFORM Y is not bound to reveal any part of the technical operation of the anti-cheat software even if this information relates to GAMER X, as long as this is can be regarded as trade secrets. The necessary balancing of interests under Art. 15(4) GDPR will have the result that the trade secrets of PLATFORM Y preclude the disclosure of this personal data because knowledge of the technical operation of the anti-cheat software could also allow the user to circumvent future cheat or fraud detection<sup>99</sup>.

174. If controllers refuse to act on a request for the right of access in whole or in part under Art. 15(4) GDPR, they have to inform the data subject of the reasons without delay and at the latest within one month (Art. 12(4) GDPR). The explanatory statement has to refer to the concrete circumstances in order to allow the data subjects to assess whether they want to take action against the refusal. It must include information about the possibility of lodging a complaint with a supervisory authority (Art. 77 GDPR) and seeking judicial remedy (Art. 79 GDPR).

### 6.3 Article 12(5) GDPR

175. Art. 12(5) GDPR enables controllers to override requests for the right of access that are manifestly unfounded or excessive. These concepts have to be interpreted narrowly, as the principles of transparency and cost free data subjects rights must not be undermined.
176. Controllers must be able to demonstrate to the individual why they consider that the request is manifestly unfounded or excessive and, if asked, explain the reasons to the competent supervisory authority. Each request should be considered on a case by case basis in the context in which it is made in order to decide if it is manifestly unfounded or excessive.

#### 6.3.1 What does manifestly unfounded mean?

177. A request for the right of access is manifestly unfounded, if the requirements of Art. 15 GDPR are clearly and obviously not met when applying an objective approach. However, as explained especially in section 3 above, there are only very few prerequisites for requests for the right of access. Therefore, the EDPB emphasises that there is only very limited scope for relying on the “manifestly unfounded” alternative of Art. 12(5) GDPR in terms of requests for the right of access.
178. Furthermore, it is important to recall that prior to invoking the restriction, controllers must carefully analyse the content and scope of the request. For example, a request should not be regarded as manifestly unfounded if the request is related to the processing of personal data not subject to the GDPR (in this case, the request should not be dealt with as an Art. 15-request at all).

---

<sup>99</sup> The extent of the information provided to individuals will be heavily context dependent, taking into account the nature of the controller and the nature of the breach of the terms of service. In some cases, it may only be possible for the controller to provide basic information in response to an access request to which Art. 15(4) applies.

179. Other cases in which the applicability of Art. 12(5) GDPR is questionable are requests related to information or processing activities that are clearly and obviously not subject to the processing activities of the controller.

**Example 38:** A data subject addresses a request to a municipal authority concerning data that are processed by a state authority. Instead of arguing that the request is manifestly unfounded it would be more suitable as well as easier for the authority addressed to confirm that these data are not being processed by the authority (first component of Art. 15 GDPR: “whether” personal data are being processed)<sup>100</sup>.

180. A controller should not presume that a request is manifestly unfounded because the data subject has previously submitted requests which have been manifestly unfounded or excessive or if it includes unobjective or improper language.

### 6.3.2 What does excessive mean?

181. There is no definition of the term “excessive” in the GDPR. On the one hand, the wording “in particular because of their repetitive character” in Art. 12(5) GDPR allows for the conclusion that the main scenario for application of this limb with regard to Art. 15 GDPR is linked to the quantity of requests of a data subject for the right of access. On the other hand, the aforementioned phrasing shows that other reasons that might cause excessiveness are not excluded *a priori*.
182. Certainly, according to Art. 15(3) GDPR regarding the right to obtain a copy, a data subject may submit more than one request to a controller<sup>101</sup>. In the event of requests that could potentially be regarded as excessive, the assessment of “excessiveness” depends on the analysis carried out by the controller and the specifics of the sector in which it operates.
183. In case of subsequent requests, it has to be assessed whether the threshold of reasonable intervals (see Recital 63) has been exceeded or not. Controllers must take into account the particular circumstances of each case carefully.
184. For example, in the case of social networks, a change in the data set will be expected at shorter intervals than in the case of land registers or central company registers. In the case of business associates, the frequency of contacts with the customer should be considered. Accordingly the “reasonable intervals” within which data subjects may again exercise their right of access are also different. The more often changes occur in the database of the controller, the more often data subjects may be permitted to request access to their personal data without it being excessive. On the other hand, a second request by the same data subject could be considered to be repetitive in certain circumstances.
185. When deciding whether a reasonable interval has elapsed, controllers should consider the following in the light of the reasonable expectations of the data subject:
- how often the data is altered – is information unlikely to have changed between requests? If a data pool is obviously not subject to a processing other than storage and the data subject is

---

<sup>100</sup> A different question is whether the authority which the access request was addressed to is entitled to transmit the request to the competent state authority.

<sup>101</sup> According to the second sentence of Article 15(3), the controller may charge a reasonable fee for further copies requested.

aware of this, e.g. because of a previous request for the right of access, this might be an indication for an excessive request;

- the nature of the data – this could include whether it is particularly sensitive;
- the purposes of the processing – these could include whether the processing is likely to cause detriment (harm) to the requester if disclosed;
- whether the subsequent requests concern the same type of information or processing activities or different ones<sup>102</sup>.

**Example 39 (carpenter):** A data subject lodges access requests **every two months** with the carpenter that manufactured a table for them. The carpenter answered the first request completely. When deciding whether a reasonable interval has elapsed, one should consider that the carpenter only occasionally (first bullet point above) and not as part of its core activity processes and collects personal data and it is even less likely that the carpenter often provides services to the same data subject. Indeed, in the case, the carpenter did not provide more than one service to the data subject, rendering it unlikely that changes occurred in the dataset concerning the data subject. Notably given the nature and amount of the personal data processed, the risks related to the processing can be considered as low (second bullet point above), such as the purpose of the processing (billing purposes and compliance with obligation to keep records) is not likely to cause detriment to the data subject (third bullet point above). The request furthermore concerns the same information as the last request (forth bullet point above). Such requests may as a consequence be regarded as excessive due to their repetitiveness.

**Example 40 (social media platform):** A social media platform whose core business is the collection and/or processing of personal data of the data subject carries out large-scale complex and continuous processing activities. A data subject that uses the services of the platform lodges access requests **every three months**. In this case, frequent changes to the personal data relating to the data subject are highly likely (first bullet point above), the broad range of collected data includes inferred sensitive personal data (second bullet point above) processed for the purpose of showing relevant content and network members to the data subject (third bullet point). Access requests every three months may - under these circumstances - in principle not be regarded as excessive due to repetitiveness.

**Example 41 (credit agencies):** As with social networks, it cannot be ruled out that modifications of the relevant data held by credit agencies will occur at much shorter intervals than in other areas (first bullet point above). This results from numerous factors of which the data subject, as a person from outside, is usually not aware due to the complexity of the business model. The answer to the question as to which types of data were collected for a score value calculation by the controller and which are currently included in the calculation can therefore only be provided by the credit agency itself. In addition, data processing through credit agencies and the resulting score value can have far-reaching consequences for the data subject with regard to intended legal transactions, such as the conclusion of purchasing, rent or leasing contracts (third bullet point above).

---

<sup>102</sup> If the subsequent request concerns the same type of information in scope AND time, this is not a question of excessiveness but a question of request for an additional copy, see section 2.2.2.2.

It is not possible to generally determine any specific interval in which the submission of a further access request could be deemed excessive under Art. 12(5) second sentence GDPR. An overall consideration of the circumstances of the individual case is rather required. However, given the importance of data processing for the data subjects' reality of everyday life, it can be assumed that a **one-year interval** between information provided free of charge will in any case be too large for the request to be considered excessive. If a request is submitted within a very short interval, the decisive factor should be whether the data subject has reason to assume that the information or the processing has changed since the last request. For example, if the data subject has conducted a financial transaction, such as taking a loan, the data subject should be entitled to request access to the credit information even though such a request was submitted and responded to shortly before.

186. When it is possible to provide the information easily by electronic means or by remote access to a secure system, which means that complying with such requests actually doesn't strain the controller, it is unlikely that subsequent requests can be regarded as excessive.
187. If a request overlaps with a previous request, the overlapping request can generally be regarded as excessive, if and insofar as it covers exactly the same information or processing activities and the previous request is not yet complied with by the controller without reaching the state of "undue delay" (see Art. 12(3) GDPR). In practice, as a consequence both requests could be combined.
188. The fact that it would take the controller a vast amount of time and effort to provide the information or the copy to the data subject cannot on its own render a request excessive<sup>103</sup>. A large number of processing activities typically implicates bigger efforts when complying with access requests. However, as stated above, under certain circumstances requests can be regarded as excessive due to other reasons than their repetitive character. In the view of the EDPB this encompasses particularly cases of abusively relying on Art. 15 GDPR, which means cases in which data subjects make an excessive use of the right of access with the only intent of causing damage or harm to the controller.
189. Against this background, a request should not be regarded as excessive on the ground that:
  - no reasons are given by the data subject for the request or the controller regards the request as meaningless;
  - improper or impolite language is used by the data subject;
  - the data subject intends to use the data to file further claims against the controller.<sup>104</sup>
190. On the other hand, a request may be found excessive, for example, if:
  - an individual makes a request, but at the same time offers to withdraw it in return for some form of benefit from the controller or
  - the request is malicious in intent and is being used to harass the controller or its employees with no other purposes than to cause disruption, for example based on the fact that:

---

<sup>103</sup> No proportionality test, see above para. 166.

<sup>104</sup> This is without prejudice to any applicable national law that comply with the requirements posed by Art. 23 GDPR, see Chapter 6.4.

- the individual has explicitly stated, in the request itself or in other communications, that it intends to cause disruption and nothing else; or
- the individual systematically sends different requests to a controller as part of a campaign, e.g. once a week, with the intention and the effect of causing disruption<sup>105</sup>.

### 6.3.3 Consequences

191. In case of a manifestly unfounded or excessive request for the right of access controllers may, according to Art. 12(5) GDPR, either charge a reasonable fee (taking into account the administrative costs of providing information or communication or taking the action requested) or refuse to comply with the request.
192. The EDPB points out that controllers are – on the one hand – not generally obliged to charge a reasonable fee before refusing to act on a request. On the other hand, they aren't completely free to choose between the two alternatives either. In fact, controllers have to make an adequate decision depending on the specific circumstances of the case. Whereas it is hardly imaginable that charging a reasonable fee is a suitable measure in case of manifestly unfounded requests, for excessive requests – in line with the principle of transparency – it will often be more appropriate to charge a fee as a compensation for the administrative costs the repetitive requests are causing.
193. Controllers must be able to demonstrate the manifestly unfounded or excessive character of a request (Art. 12(5) third sentence GDPR). Hence, it is recommended to ensure proper documentation of the underlying facts. In line with Art. 12(4) GDPR, if controllers refuse to act on an access request in whole or partly, they must inform the data subject without delay and at the latest within one month of receipt of the request of
  - the reason why,
  - the right to lodge a complaint with a supervisory authority,
  - the possibility to seek a judicial remedy.
194. Before charging a reasonable fee based on Art. 12(5) GDPR, controllers should provide an indication of their plan to do so to the data subjects. The latter have to be enabled to decide whether they will withdraw the request to avoid being charged.
195. Unjustified rejections of requests of the right of access can be regarded as infringements of data subject rights pursuant to Art. 12 to 22 GDPR and can therefore be subject to the exercise of corrective powers by competent supervisory authorities, including administrative fines based on Art. 83(5)(b) GDPR. If data subjects consider there is an infringement of their data subject rights, they have the right to lodge a complaint based on Art. 77 GDPR.

---

<sup>105</sup> “Systematically sending as part of a campaign” means that requests which could easily be combined to one are artificially split into not just a few but many single pieces by the data subject with the apparent intention to cause disruption.

## 6.4 Possible restrictions in Union or Member States law based on Article 23 GDPR and derogations

196. The scope of the obligations and rights provided for in Art. 15 GDPR may be restricted by way of legislative measures in Union or Member States law<sup>106</sup>.
197. Controllers, who plan to rely on a restriction based on national law must carefully check the requirements of the provision of the respective national legislation. Furthermore, it is important to note, that restrictions of the right of access in Member States (or Union) law which are based on Art. 23 GDPR must strictly fulfil the conditions laid down in this provision. The EDPB has issued the Guidelines 10/2020 on restrictions under Art. 23 GDPR with further explanations on this. In terms of the right of access, the EDPB recalls that controllers should lift the restrictions as soon as the circumstances that justify them no longer apply<sup>107</sup>.
198. Legislative measures which relate to restrictions under Art. 23 GDPR may also foresee that the exercise of a right is delayed in time, that a right is exercised partially or circumscribed to certain categories of data or that a right can be exercised indirectly through an independent supervisory authority<sup>108</sup>.

---

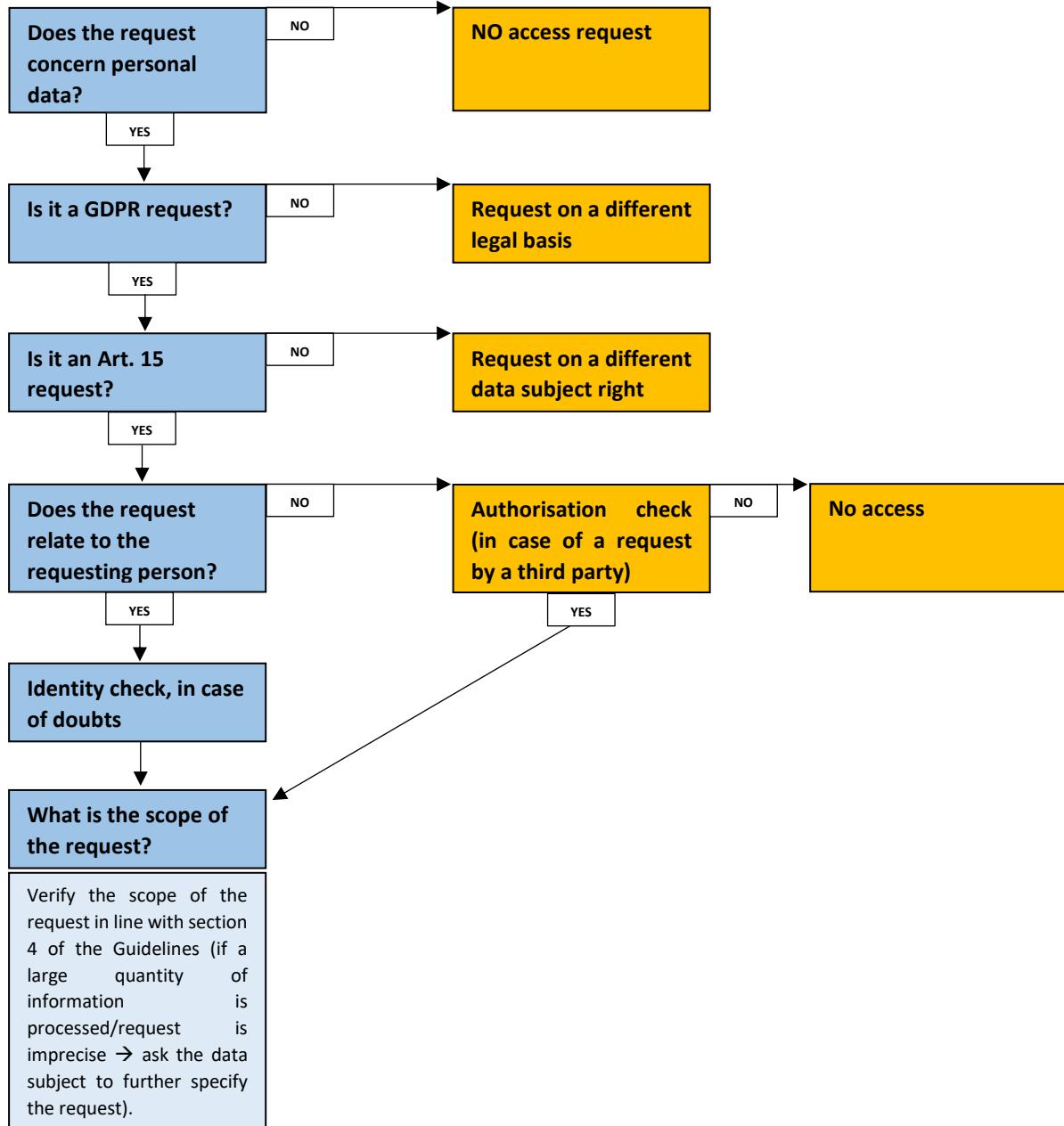
<sup>106</sup> See for example sections 32 to 37 of the German Federal Data Protection Act (BDSG), sections 16 and 17 of the Norwegian Personal Data Act and chapter 5 of the Swedish Data Protection Act.

<sup>107</sup> Paragraph 76 of the Guidelines 10/2020 on restrictions under Art. 23 GDPR, Version 2.0, adopted on 13 October 2021.

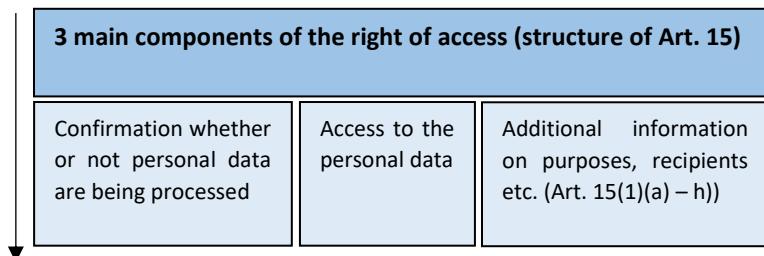
<sup>108</sup> Paragraph 12 of the Guidelines 10/2020 on restrictions under Art. 23 GDPR, Version 2.0, adopted on 13 October 2021. Section 34 (3) of the German Federal data protection act for example states that if a public authority doesn't provide information to a data subject complying with a request for the right of access because of certain restrictions, such information shall be provided to the federal supervisory authority at the request of the data subject, unless the responsible supreme federal authority (of the authority which was subject to the request) determines in the individual case that doing so would endanger the security of the Federation or a Land. The Italian DPCode provides for indirect access (through the authority) in case the access could impact with adverse consequence on a number of interests (e.g. Interest to contrast money laundering) see Art. 2-L of the Italian DPCode.

## ANNEX – FLOWCHART

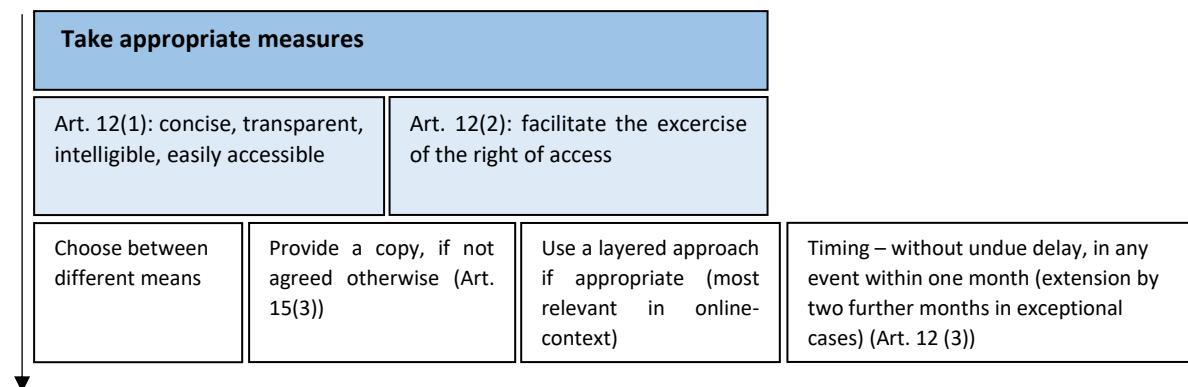
### Step 1: How to interpret and assess the request?



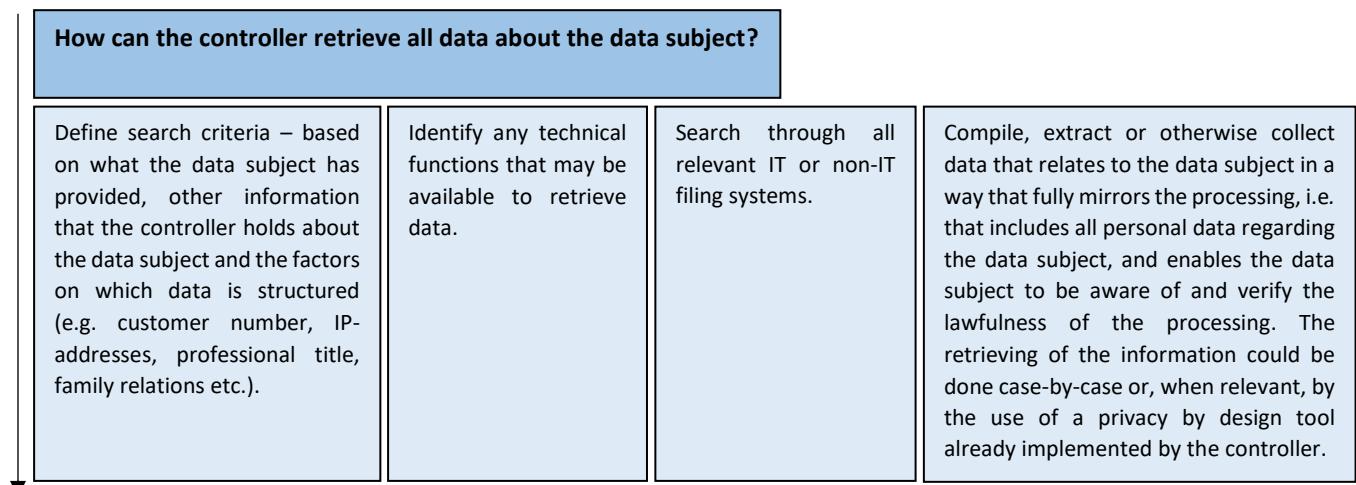
## Step 2: How to answer the request (1)?



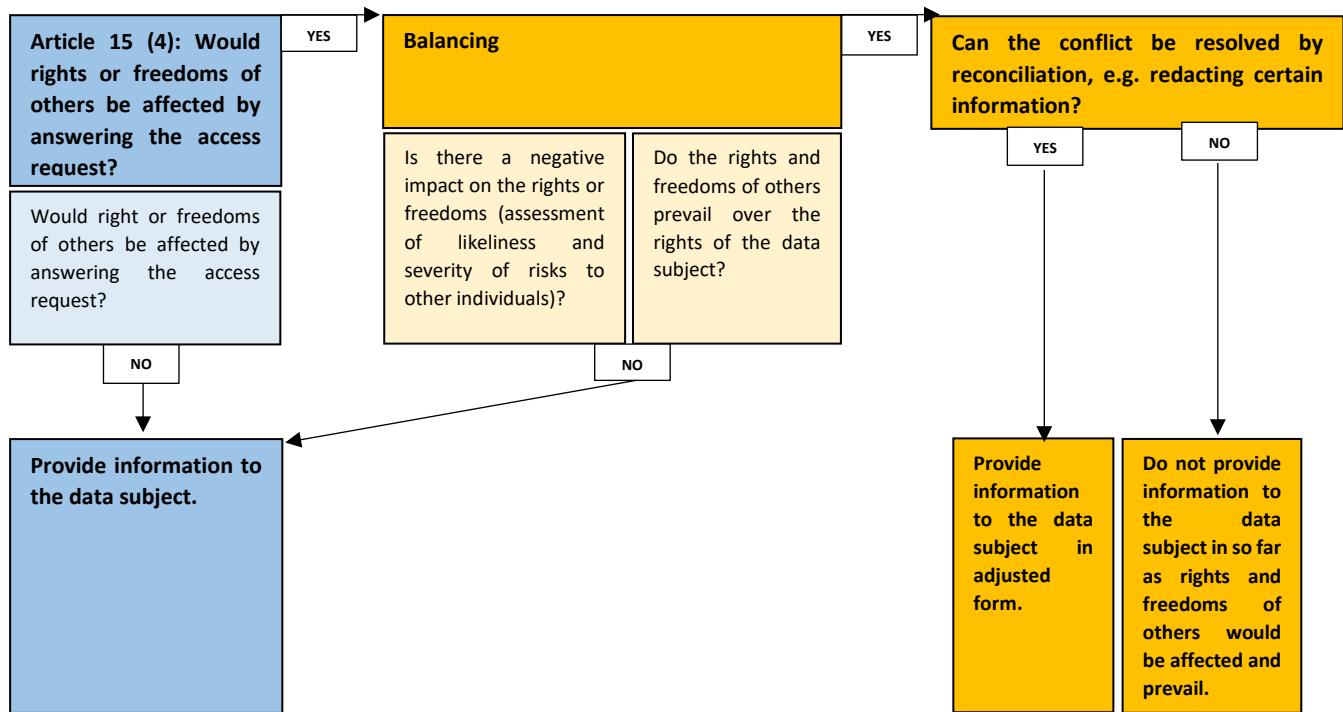
## Step 2: How to answer the request (2)?



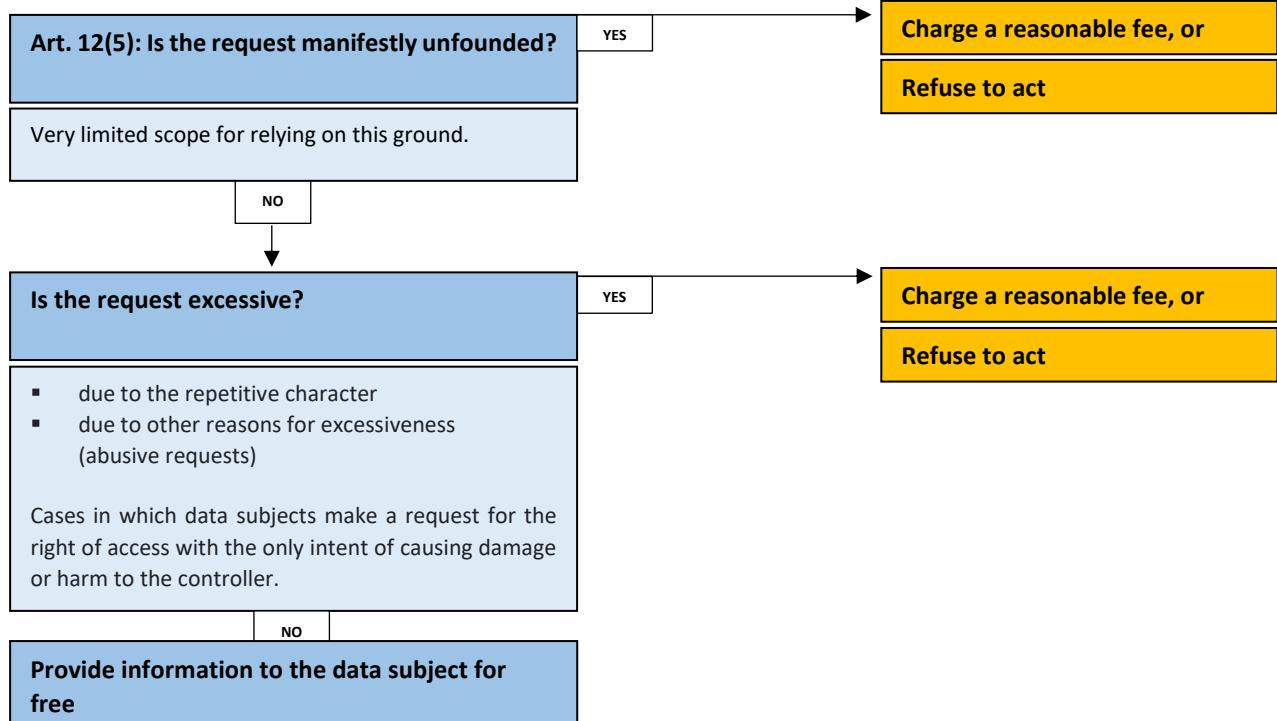
## Step 2: How to answer the request (3)?



### Step 3: Checking limits and restrictions (1)



### Step 3: Checking limits and restrictions (2)



# Guidelines



## **Guidelines 06/2022 on the practical implementation of amicable settlements**

**Version 2.0**

**Adopted on 12 May 2022**

## Version history

Version 2.0	12 May 2022	Adoption of Guidelines 06/2022 Only minor editorial adjustments were made in comparison to Version 1.0, for the purpose of publication.
Version 1.0	18 November 2021	Adoption of Internal EDPB Document 06/2021 The EDPB members decided to discuss the publication of the document after a period of 6 months, allowing the EDPB members to gain experience from practice during that time

## Table of contents

1	SCOPE AND AIM .....	4
2	DEFINITION OF THE TERM “AMICABLE SETTLEMENT”.....	5
2.1	General context.....	5
2.2	GDPR context.....	6
2.3	The aim of amicable settlements in general .....	8
3	GENERAL LEGAL ANALYSIS .....	9
3.1	The power to reach an amicable settlement as one of the powers vested in SAs .....	9
3.2	The amicable settlement procedure in the OSS context .....	10
3.2.1	Amicable settlement achieved by the complaint-receiving CSA in the preliminary vetting phase .....	10
3.2.2	Amicable settlement attempted by the LSA .....	11
3.2.3	Cases under Article 56(2) .....	15
4	LEGAL CONSEQUENCES AND PRACTICAL RECOMMENDATIONS .....	16
4.1	Application of the principle of good administration to the amicable settlement procedure in the OSS context.....	16
4.2	The cooperation procedure following an amicable settlement achieved by the LSA .....	17
4.3	Amicable settlement in Article 56(2) cases .....	18
	Annex 1: RELEVANT STEPS WHEN HANDLING A CASE VIA AMICABLE SETTLEMENT .....	19
	Annex 2: COUNTRIES WHERE AMICABLE SETTLEMENTS ARE NOT POSSIBLE IN ACCORDANCE WITH THE NATIONAL LEGISLATION.....	22

# The European Data Protection Board

Having regard to Article 70(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"),

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<sup>1</sup>,

Having regard to Article 12 and Article 22 of its Rules of Procedure,

## HAS ADOPTED THE FOLLOWING GUIDELINES

### 1 SCOPE AND AIM

1. Practice has shown that many supervisory authorities (hereinafter "SAs") apply the instrument of amicable settlement when dealing with complaints. It is as well noticeable that there are diverse variations of amicable settlements and that they are therefore handled differently by SAs due to differing domestic legislations. The GDPR uses the term "amicable settlement" only in Recital 131 in reference to the handling of local cases under Article 56(2) GDPR, but does not explicitly limit the possibilities to facilitate such local cases. The resulting lacuna in regulation of amicable settlements for non-local cases has been filled in divergent ways, some by way of Member State law, others by way of interpretation. Given these different interpretations and given the differing national laws governing complaint handling and amicable settlements (if at all present), the practical implementation of the instrument of amicable settlements differs considerably among Member States.
2. The powers of the SAs should be exercised in accordance with specific requirements in their Member State procedural law. This applies also to the handling of cases. However, national procedural law must comply with the principles of equivalence and effectiveness and may hence not render excessively difficult or practically impossible the exercise of the rights conferred by EU law (i.e. the GDPR). Through these Guidelines, the EDPB therefore seeks to provide best practices for a consistent application of the GDPR at national and EU level, to the extent appropriate for the application of the instrument of amicable settlement, taking into account the various national procedural legislations – insofar as such an instrument has been implemented explicitly – the procedure of the OSS mechanism under the GDPR, and the technical environment (IMI).
3. Cases handled by SAs can have origins other than complaints, for example cases based on media reports or ex officio investigations. However, the present guidance will address the practical

---

<sup>1</sup> References to "Member States" made throughout these Guidelines should be understood as references to "EEA Member States".

implementation of amicable settlements only for cases that originated as a complaint from a data subject since the possibility of a settlement postulates the existence of a dispute between two entities, in this case the complaint lodged by a data subject against a data controller (see also paragraph 2.1 below). Furthermore, such complaints can be divided into (i) national cases without cross-border character, (ii) cases where the OSS mechanism applies because the case is cross-border in nature, and (iii) cross-border cases that are handled locally pursuant to Article 56(2) GDPR. Again, even though practice shows that amicable settlements are a possible course of action for all situations, the present guidance will mainly address those complaints that are cross-border in nature.

## 2 DEFINITION OF THE TERM “AMICABLE SETTLEMENT”

### 2.1 General context

4. The GDPR does not define the meaning of the term “amicable settlement” and only refers to this expression in Recital 131.<sup>2</sup> The most relevant meanings of “settlement” are “an arrangement” and “an official agreement intended to resolve a dispute or conflict”. The Oxford English Dictionary explains the adjective “amicable” as “characterised by friendliness and absence of discord”.
5. The way amicable settlements are defined more generally in the legal profession and throughout other international documents provides some preliminary guidance for determining the definition of amicable settlements. For example, the International Chamber of Commerce (“ICC”) provides a range of dispute resolution procedures that may be considered “amicable settlements”.<sup>3</sup> The principle amicable settlement procedure at the ICC appears to be mediation, which is described as a “flexible and consensual technique in which a neutral facility helps the parties reach a negotiated settlement of their disputes.” According to the ICC, such settlements achieved through mediation are contractually binding and widely enforceable. The World Trade Organization (“WTO”) uses amicable settlements as “mutually agreed solutions”, which constitutes a “negotiated solution” between the involved parties that allows for swift and tailored solution of a dispute.<sup>4</sup> Moreover, the European Union Intellectual Property Office (“EUIPO”) refers to amicable settlements as a “process outside of the court resulting in

---

<sup>2</sup> Recital 131 : “<sup>1</sup>Where another supervisory authority should act as a lead supervisory authority for the processing activities of the controller or processor but the concrete subject matter of a complaint or the possible infringement concerns only processing activities of the controller or processor in the Member State where the complaint has been lodged or the possible infringement detected and the matter does not substantially affect or is not likely to substantially affect data subjects in other Member States, the supervisory authority receiving a complaint or detecting or being informed otherwise of situations that entail possible infringements of this Regulation should seek an amicable settlement with the controller and, if this proves unsuccessful, exercise its full range of powers. <sup>2</sup>This should include: specific processing carried out in the territory of the Member State of the supervisory authority or with regard to data subjects on the territory of that Member State; processing that is carried out in the context of an offer of goods or services specifically aimed at data subjects in the territory of the Member State of the supervisory authority; or processing that has to be assessed taking into account relevant legal obligations under Member State law.”

<sup>3</sup> <https://iccwbo.org/dispute-resolution-services/mediation/icc-international-centre-for-adr/>.

<sup>4</sup> Wolfgang Alschner, Amicable Settlements of WTO Disputes: Bilateral Solutions in a Multilateral System, World Trade Review, Volume 13 (1), 2014, p. 65-102.

a solution negotiated between the parties [...] through mediation".<sup>5</sup> The European Consumer Center ("ECC") also refers to amicable settlements<sup>6</sup> as a form of "alternative dispute resolution procedures", as laid down in the Directive on alternative dispute resolution for consumer disputes<sup>7</sup>, as procedures that are "provided by neutral out-of-court bodies such as conciliators, mediators, arbitrators, the ombudsman and complaints boards",<sup>8</sup> and in which "consumers and businesses attempt to resolve a dispute jointly [...] by hearing both parties, examining the legal situation, discussing possible solutions and finally making a proposal for arbitration".<sup>9</sup>

6. All in all, it appears that amicable settlements generally refer to alternative dispute resolutions through proceedings that result in the cordial closure of a case. Whereas a settlement between the parties is the outcome, the proceeding itself follows an amicable approach. The procedures can range from party-to-party negotiations to formal mediations and even facilitated conciliation practices.

## 2.2 GDPR context

7. In the context of complaint handling by data protection authorities, most Member States see amicable settlements as a process of "alternative dispute resolution". In most cases, the amicable settlement is facilitated where a complaint is lodged with the SA concerning the alleged violation of the GDPR, in particular concerning data subjects' rights, to resolve the case in the data subjects' favour. In such cases, the settlement is to be reached between the controller and the data subject, under the supervision of the SA, which moderates the course of events. Thus, the SA acts as a sort of facilitator of the process aimed at settling the complaint. The SA, unlike an actual "mediator", takes an active part in the proceeding as it still has to fulfil its obligations as SA and is therefore required to handle the complaint, to investigate the subject matter of the complaint with its specifics to an appropriate extent, and to inform the data subject on the progress or the outcome regarding the complaint.
8. Given the relative silence of the GDPR on amicable settlements, which alternative dispute resolution process is followed and the requirements and conditions that govern that process, will largely depend on each particular Member State's law and policy. An analysis of standing practice shows that, when dealing with amicable settlements, the majority of the national legal systems include the receiving SA, the controller (or processor) and the data subject in the proceeding, as well as, if applicable, also the Lead Supervisory Authority (LSA).
9. It should be noted that in some Member States, the data subject is not a party to the administrative

---

<sup>5</sup> EUIPO, Decision No. 2013-3 of the Presidium of the Board of Appeal of 5 July 2013 on the amicable settlement of disputes ("Decision on Mediation"), <https://euipo.europa.eu/ohimportal/en/mediation#>.

<sup>6</sup> [https://europa.eu/youreurope/citizens/consumers/consumers-dispute-resolution/informal-dispute-resolution/index\\_en.htm](https://europa.eu/youreurope/citizens/consumers/consumers-dispute-resolution/informal-dispute-resolution/index_en.htm)

<sup>7</sup> Directive 2013/11/EU on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC

<sup>8</sup> [https://europa.eu/youreurope/citizens/consumers/consumers-dispute-resolution/out-of-court-procedures/index\\_en.htm](https://europa.eu/youreurope/citizens/consumers/consumers-dispute-resolution/out-of-court-procedures/index_en.htm)

<sup>9</sup> E.g. the German equivalent website <https://www.evz.de/einkaufen-internet/odr-adr/beratung-schlichtung.html>

proceedings against the controller. In such Member States, the SA may use a similar dispute resolution process to what is described in these Guidelines and close a case if it deems that the controller has fulfilled the claims, but without hearing the data subject. Such resolution processes will however not be addressed in these Guidelines.

10. Amicable settlements are mainly regarded to be possible at any stage of a proceeding, even though some SAs indicate that they are only possible in the early stages of case consideration, before any other action has been taken. In some Member States, amicable settlements are only applicable in local cases, due to the fact that the GDPR uses this term only in Recital 131, where an approach by the Concerned Supervisory Authority (CSA) in local cases is described accordingly. However, the majority of the SAs declare the instrument of an amicable settlement permissible in any kind of cases, regardless of their cross-border or otherwise local nature.
11. Regarding Recital 131, the scope for such agreements is limited to cases in which the CSA receiving the complaint finds that the concrete subject matter or the possible infringement concerns only processing activities of the controller or processor in the Member State where the complaint has been lodged, or (likely) does not substantially affect data subjects in other Member States. The choice whether to seek an amicable settlement should then include, as the Recital states, (i) the specific processing carried out in the territory of the Member State or with regard to data subjects on the territory of that Member State, (ii) processing that is carried out in the context of an offer of goods or services specifically aimed at data subjects in the territory of the Member State, or (iii) processing that has to be assessed taking into account relevant legal obligations under Member State law. Legislations explicitly allowing amicable settlements, on the other hand, may not be limited to these requirements.
12. In principle, the choice whether an amicable settlement may or may not be pursued depends on Member State law and/or the discretion of the SA involved. Regarding the criteria on the basis of which cases may be considered appropriate for amicable resolution, such criteria could on the one hand include the manner in which the SA has come to know of the case. The procedure of an amicable settlement could therefore only be deemed applicable in cases where a complaint has been lodged.
13. Amicable settlements should in general only be considered possible in cases concerning the data subjects' rights laid down in Articles 12 et seq. of the GDPR, given that only then the data subject can dispose of his or her own rights as a party to the settlement. However, with due regard to national legislation of individual Member States, such decision is subject to the discretion of the SA as it has to assess the broader picture of the individual case.
14. On the other hand, the factual circumstances of the case could be decisive. Such special circumstances under which it is determined whether an amicable settlement may or may not be conducted can be governed by national regulations, whereas the GDPR remains silent on the matter (apart from Recital 131). In practice, the following general criteria could guide the SA in taking the decision to initiate an amicable settlement procedure: There is a likelihood for the case to be solved amicably at all; only a limited amount of data subjects is affected and whether or not there is a systemic failure

recognisable;<sup>10</sup> the data protection violation is incidental or accidental (in the sense of negligence); the case involves the processing of a limited number of personal data; the effects of the violation are not of serious duration and nature (meaning that there are no severe consequences or infringements of freedoms and rights). Moreover, the likelihood of further violations in the future might be a determining factor. In addition, the broader societal significance and public interest of enforcement action on the part of the SA, also in light of any identified areas of special vigilance, as well as the extent to which an SA is able to take effective and efficient action can be decisive.

**Example 1:**

A controller or processor accepts to provide any information requested by a supervisory authority to resolve a complaint, such as clear proof that it has complied with Articles 33 and 34 of the GDPR in case of a personal data breach. The reason why the request was not fulfilled right away (in line with Article 12 GDPR) was based on a discrepancy in the internal communication process.

15. Notwithstanding, it is important to note that any SA has the right to further investigate the issue even after an amicable settlement has been reached, albeit in a different or other procedure on own volition. The authority may continue the proceedings ex officio if, for example, it considers that a fine should be imposed or receives other similar complaints about the same controller, leading to the conclusion that the controller has not fulfilled their commitment to remedy data protection violation(s), or if the complaint and/or the investigations reveal other, possibly systemic infringements that may have wider consequences or impacts on other data subjects. The same applies when the amicable settlement concerns only parts of a complaint, whereas other or additional issues of the case are handled otherwise. Furthermore, an amicable resolution does not preclude the data subject from reverting to the SA, should it turn out (later) that the data controller did not comply with their resolution as agreed. These circumstances should be communicated in a clear and transparent way to the controller and to the complainant before an amicable settlement is reached.

**Example 2:**

The data subject makes a complaint that a controller is seeking a passport as a means of identification in order to delete an account held by the data subject on the controller's platform. The SA deems the individual complaint suitable for attempted amicable settlement, in that the data subject may be satisfied if the demand for a passport is rescinded, and the account deleted. However, the SA opens an own-volition inquiry into the controller's policies around data processing in respect of platform accounts, in order to ensure that the controller brings its policies into compliance with the provisions of the GDPR.

## 2.3 The aim of amicable settlements in general

16. In addition to reaching an outcome which is satisfactory for the data subject, amicable settlements are tools to achieve compliance with the GDPR by the controller. In case a complaint is lodged because a

---

<sup>10</sup> Cf. Example 2 below regarding this criterion.

controller has not fulfilled the data subject rights pursuant to Articles 12 to 22 GDPR, the enforcement of data subject rights can be expedited by an amicable arrangement between the actors. The yardstick against which the successful amicable resolution of the complaint is measured should include two elements: on the one hand, the satisfaction of the data subject achieved in the specific case in relation to the specific issues raised in the complaint and, on the other hand, where applicable and required by national law, the proof provided by the controller to the SA that it has met the data subject's requests and complied with the applicable data protection requirements. However, the SA should determine in practice, and by having regard to the circumstances of the case and to the given cooperation with other SAs involved in the case, whether the amicable settlement is enough to achieve full compliance with the GDPR in the light of the legal issues surrounding or arising from the individual complaint against the individual controller.

17. Thus, amicable settlements should be understood broadly as one of the options for an SA to address data subjects' complaints and ensure the protection of data subject rights. At the same time, it must be recognized that amicable settlements may not be an appropriate solution for every case. While it is for the SAs themselves to determine whether an amicable settlement may or may not be pursued in a given case, such assessment must be carried out on the basis of structured, uniform, transparent and explainable criteria, such as the ones mentioned in paragraph 12 et seq., and taking into account provisions of national law, where existent.
18. The SA's corrective powers are of paramount importance for the enforcement and maintenance of the high level of protection which the GDPR seeks to create for all data subjects, who are often in a difficult or even dependent position vis-à-vis the controller. Resolving a dispute through the procedure of amicable settlements with an SA handling the process comparable to a facilitator can then be a way to address and handle such imbalance and to find a solution that is acceptable for each party, especially the data subject as regards the fulfilment of his or her rights.

### 3 GENERAL LEGAL ANALYSIS

#### 3.1 The power to reach an amicable settlement as one of the powers vested in SAs

19. An amicable settlement procedure finds its legal basis in the tasks directly conferred on SAs by the GDPR (Article 57(1)(a) and (f) GDPR) and additionally in the powers granted to SAs by a national law within the framework of Article 58(6) GDPR, where this exists.
20. In the first case, Article 57(1)(a) and (f) GDPR generally apply, providing sound foundations for a SA to seek all possible avenues to "handle" complaints (see paragraph 1(f) of Article 57) and "enforce" (see paragraph 1(a) of Article 57) the application of the Regulation as appropriate. Article 57(1)(f) read in conjunction with Article 77 and 78 implies an individual right to have every complaint (if admissible) handled and investigated to the extent necessary to reach an outcome appropriate to the nature and circumstances of that complaint. However, it falls within the discretion of each competent supervisory authority to decide the extent to which a complaint should be investigated. An outcome could e.g. be

that the parties to the complaint through the intervention of the SA have settled the case amicably.

21. SAs may, in the second scenario, be empowered by Member States to exercise additional powers pursuant to national law, as per Article 58(6) GDPR. The specifics of operational case handling matters for a SA (including a LSA) to reach an amicable resolution are to be found in these national provisions.

### 3.2 The amicable settlement procedure in the OSS context

22. In order to assess the role of the amicable settlement in the context of the OSS procedure, reference can be made in the first place to the rationale of such procedure as set out in Article 60(1) GDPR. As clarified in the EDPB Guidelines 02/2022 on the application of Article 60 GDPR<sup>11</sup>, “Article 60(1) lays down basic and overarching principles, which apply throughout the entire cooperation between SAs. In accordance with the wording of this Article, the key concepts of the cooperation procedure consist of ‘an endeavour to reach consensus’ and the obligation to ‘exchange all relevant information.’” Furthermore, “[...] these obligations are to be complied with by the LSA and every CSA (mutual obligation).”

#### 3.2.1 Amicable settlement achieved by the complaint-receiving CSA in the preliminary vetting phase

23. The EDPB wishes to point out that although amicable settlement is only mentioned in the context of Recital 131, seeking for an amicable settlement may also be a good practice when an SA is handling a case that does not fulfil the conditions laid down by Article 56.2 GDPR, depending on the national procedural legislation.
24. Recital 131 as such does not prevent the CSA receiving a complaint from attempting, as part of the preliminary vetting, to seek such a settlement in addition to establishing the “fully” cross-border nature of that complaint. Nevertheless, the specific approach may depend on whether the controller has an establishment on the territory of that receiving SA or not. As already clarified in Section 2, an inherent feature of amicable settlement is the mutual satisfaction of the parties involved, most particularly the complainant. If this is the case and the CSA can objectify such a satisfaction in advance, in the vetting phase of the complaint, after e.g. the controller complied with the data subjects rights request to the satisfaction of both the data subject and the receiving SA, the receiving SA should no longer inform the LSA of the case through an Article 56 IMI notification, as the object of the complaint is no longer present. Accordingly, there is no need to start an OSS procedure by uploading the case to the IMI.
25. According to Recital 125 the LSA is generally competent for adopting any legally binding decision on the relevant controller or processor in an OSS context. Moreover, under Article 56(6) GDPR, the LSA is the “sole interlocutor” of the controller/processor for the cross-border processing in question. Therefore, the receiving SA should communicate the case and outcome to the LSA at an appropriate

---

<sup>11</sup> Paragraphs 37 and 38 of the EDPB Guidelines 02/2022 on the application of Article 60 GDPR.

time, for instance on a quarterly basis (i.e.: through the voluntary mutual assistance), in line with the cooperation requirement that is inherent in the whole OSS mechanism, in order for the LSA to be able to take any action it deems appropriate in respect of the given controller.

26. This means that the LSA should be kept informed about the successful amicable settlements achieved by the CSA in such a preliminary phase, also in aggregate format. More specific guidance in this respect is provided in Section 4 below ('Recommendations').
27. Needless to say, there are cases where the settlement achieved by the CSA with the controller/processor may be only a partial one, i.e. not all the requests are granted, so that the involvement of the LSA becomes indispensable with a view to providing all the remedies envisaged by the GDPR to the data subject.
28. **LEGAL CONSEQUENCES:** The amicable settlement that a CSA is empowered to achieve as part of the preliminary vetting activity in respect of the received complaint may make it unnecessary to initiate an Article 60 procedure insofar as the settlement achieved is to the full satisfaction of the parties involved. If this is not the case and due to the principle to the right to good administration in Art. 41 EUChFR which also applies to OSS cases, the LSA should then consider the reasons why the amicable settlement could not be reached within the preliminary phase by the CSA and decide whether another attempt could lead to a conclusion of the complaint within a reasonable time.

### 3.2.2 Amicable settlement attempted by the LSA

29. Where the LSA decides to attempt an amicable settlement after receiving the case, a key requirement to be met stems, once again, from the rationale of the OSS cooperation procedure, i.e. the need for CSAs and LSA to cooperate in an endeavour to reach consensus.
30. It is important to state that the EDPB acknowledges that, in any stage of the proceeding, the LSA is at liberty to give a formal hearing to the data subject (through the complaint-receiving CSA as interlocutor) and, with the agreement of all parties involved (e.g. the data subject, the controller, the CSA(s) and possibly third parties), to close a case after the alleged infringement has been rectified even in the absence of specific domestic regulation. The LSA may do so if it considers the information gathered from the case investigations sufficient to bring the case to such form of closure. This form of settlement could be understood as a due diligence approach due to the margin of discretion in determining the conditions and requirements in case handling, as it provides a solution that enables SAs to maintain the high level of protection that the GDPR seeks to create by recognising that some cases can be solved efficiently by facilitating interaction between the parties. It can carry advantages for the complainant, whose rights under the GDPR are vindicated swiftly, as well as for the controller, who is provided the opportunity to bring its behaviour into compliance with the GDPR.
31. This means that the LSA should be mindful of the need to keep the CSAs in the loop at all stages of the proceeding. Indeed, whilst the LSA is unquestionably the sole interlocutor for the controller involved

(see, again, Article 56(6) GDPR), the complainant has his or her one-stop-shop in the competent CSA that received his or her complaint.

32. This mutual exchange of information is also a means to ensure compliance with due process and the right of the complainant to be heard in the procedure attempted by the LSA, partly with a view to submitting his or her views on top of the information already provided by the CSA. This is where the LSA's role is key in acting as the facilitator of the whole process through the exchange of information and documents with the CSA. It should also be recalled that the LSA's discretion in handling the complaint by way of an attempt at achieving an amicable settlement between the data subject and the controller is bound to be impacted by the information and documents exchanged under Article 60(1) GDPR, especially if the CSA has already unsuccessfully attempted such an amicable settlement in the vetting phase.
33. Indeed, the LSA choosing the amicable settlement as a way to resolve the dispute with the controller should be mindful of the likelihood for such an approach to lead to a successful outcome, i.e. to the vindication of the data subject's rights, in the light of all the relevant circumstances, including the expectations of the CSA that has transferred the complaint to it under the requirements of Article 56(1) GDPR. Where a CSA communicates under Article 60(1), in particular, that such an attempt has already been made unsuccessfully in the vetting phase, whether on account of the data subject's refusal to accept the settlement with the controller or on account of the controller's failure to reply to the CSA's invitation to comply with the data subject's request, the LSA should consider very carefully whether a new attempt to settle the complaint amicably does serve the interests of the data subjects, and data protection law in general. A more formalised approach in which the LSA exerts all its authority vis-à-vis the controller also under Article 58 GDPR might be the preferable action. The same applies if the CSA has made no such attempt prior to transferring the complaint to the LSA, on whatever grounds, and has accordingly communicated nothing in this respect to the LSA. In both cases, the attention paid by the LSA to the likelihood for success of the amicable settlement option will enable the LSA to select the most appropriate way for tackling the case at hand, reducing unnecessary administrative burden and avoiding the risk of resource intensive OSS procedures to address the concerns and doubts, or even the reasoned and relevant objections, of the CSA(s).
34. If the LSA comes to the conclusion that an amicable settlement is appropriate in the case at hand, it will have to consider that the settlement is part of an OSS procedure and will have to act accordingly. The EDPB has already clarified in the Article 60 Guidelines, that "in order to facilitate the reaching of consensus, the information should be shared at a moment where it is still possible for the LSA to take on board the viewpoints of the CSAs. This [...] should prevent CSAs from being presented with accomplished facts, for example because certain stages of the proceedings may be precluded under national law."<sup>12</sup>
35. In the context of an amicable settlement procedure, this means that the LSA is expected to share the

---

<sup>12</sup> Paragraph 55 of the EDPB Guidelines 02/2022 on the application of Article 60 GDPR.

proposed settlement with the CSA(s) prior to finalising it, pursuant to Article 60(3), first sentence. As pointed out by the EDPB in the Article 60 Guidelines, “[...] the CSAs’ involvement in the cooperation procedure is not limited to the right to express a relevant and reasoned objection pursuant to Article 60(4). In particular, before the creation of the draft decision the CSAs should be able to contribute to the overall procedure and may express their views also before the creation of the draft decision.”<sup>13</sup>

36. Clearly it is left to the LSA’s discretion, in light of all the factors mentioned in the foregoing paragraphs, to establish whether an informal consultation of the CSA(s) is indeed necessary in the case at hand. As recalled above in paragraphs 12 et seq., the features of the complaint lending itself to be settled amicably may arguably enable the LSA and the CSA, based also on the information exchanged beforehand under Article 60(1) at the time the complaint is transferred to the LSA, to already form their views as to the possibility of settling the complaint to the full satisfaction of the complainant by removing the cause of the dispute at its root. In such a case, the LSA may well determine that the settlement of the complaint can be directly the subject of the draft decision to be submitted under Article 60(3) GDPR. Where the CSA communicated that no settlement was achieved successfully by it in the vetting phase or that it simply did not attempt any settlement prior to transferring the case to the LSA, the LSA should conversely be mindful of the consensus objective of the OSS procedure and seek such an informal consultation of the CSA(s) beforehand to assess whether an (or another) attempt could lead to a conclusion of the complaint in a reasonable manner.
37. Ultimately, the LSA will be required to submit a draft decision to the CSAs setting out the terms of the settlement (including the steps demonstrably taken by the data controller/processor to grant the requests made by the complainants to their full satisfaction) in accordance with Article 60(3) GDPR. As clarified in the Article 60 guidance, the LSA is required to submit a draft decision to the CSAs in all cases, also when complaints are withdrawn by the complainant after the Article 60 procedure has been initiated or where no material (final) decision is issued according to national law.<sup>14</sup> The same applies when cases are (only) deemed to be withdrawn, e.g. following national law. In such a case, the draft decision serves as a final coordination between all supervisory authorities involved in the OSS procedure.<sup>15</sup>
38. As stated above, the draft decision will serve to consolidate the settlement achieved by the LSA with the agreement of the CSAs. It will be a ‘sui generis’ decision finding that the complaint has been settled by the LSA with the mutual satisfaction of the parties involved (particularly data subject, data controller), whereby such satisfaction will have to be signalled in line with the requirements of the LSA’s national law, and that the handling of the case will be terminated accordingly. Indeed, the complaint is neither dismissed nor rejected by the LSA, but it is not granted either; the amicable settlement achieved represents from this standpoint a different outcome to terminate the complaint handling procedure in the OSS context by way of an agreement between the parties that eliminates the cause of the litigation through the action taken by the LSA.

---

<sup>13</sup> Paragraph 93 of the EDPB Guidelines 02/2022 on the application of Article 60 GDPR.

<sup>14</sup> Paragraph 99 of the EDPB Guidelines 02/2022 on the application of Article 60 GDPR.

<sup>15</sup> Paragraph 100 of the EDPB Guidelines 02/2022 on the application of Article 60 GDPR.

39. With the formal submission of such an instrument as necessitated by the OSS procedure for legal certainty and transparency reasons, the 4-week period for reactions by the CSA(s) pursuant to Article 60(4) GDPR will start. In this respect, it should be emphasized that if proper exchange of information took place before the submission of the draft decision as explained in the foregoing paragraphs, and the CSA(s) never indicated any doubts that the complaint could be settled amicably, also in the spirit of cooperation, they should carefully consider whether they intend to raise objections to the finding of the achieved settlement.
40. This is not to say that CSAs are barred from raising reasoned and relevant objections in these situations; however, the whole rationale of an amicable settlement lies in achieving substantiated satisfaction of the data subject (and the controller) timely and on the basis of a mutual agreement whose chance of success in the OSS context is gauged by the LSA in the light of several factors as recalled above. All in all, reasoned and relevant objections should be exceptional in amicable settlement cases, if the consensus objective has been taken into due account by the LSA in handling the procedure; thus, rounds of revised draft decisions and/or dispute resolutions could (and should) be avoided.
41. If there are no (longer) reasoned and relevant objections, the procedure leads to the situation under Article 60(6), i.e. the draft decision will become binding on the LSA and the CSAs. Subsequently, as per Article 60(7), the lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be including a summary of the relevant facts and grounds. The CSA with which the complaint had been lodged shall inform the complainant on the decision.
42. It was explained in paragraph 15 above that the amicable settlement is not intended necessarily to cover the whole of the subject matter of a complaint, i.e. there may be parts of a complaint that the LSA does not find amenable to being settled amicably. As already pointed out in paragraphs 33 et seq., this would probably require that LSA to carefully consider whether an amicable settlement is at all appropriate even for the other parts. Nevertheless, should the LSA find that it is appropriate to settle certain parts of a complaint and proceed with handling the remaining queries by way of a 'standard' (i.e. non-amicable) approach, this will clearly reflect on the whole procedure and its outcome.
43. The different options at issue in such a composite situation will have to be represented to the CSAs prior to uploading the draft decision, which will then have to contain reasoning as to which aspects of the complaint were settled finally by way of the amicable settlement and which aspects led the LSA to dismiss or reject, or else grant, the data subject's requests. For the latter aspects (i.e. partial rejection/dismissal), the subsequent steps of the OSS procedure will be regulated by Article 60(9) GDPR. The LSA may also decide that those other parts of the complaint will need to be investigated further, and may therefore propose different solutions to the CSA(s), including the opening of a separate own volition procedure for those parts; this will have to be referenced clearly in the information accompanying the draft decision as well.

**Example 3:**

In a complaint received and vetted by the CSA the data subject alleges that the controller did not reply to his request to exercise his right of access to his personal data under Article 15 GDPR and accordingly did not enable him to request rectification under Article 16 GDPR of what he believes is inaccurate information held concerning him. The CSA did not attempt to settle the complaint amicably. The LSA receiving the complaint from the CSA considers that there is room for attempting an amicable settlement in light of the relevant features; it then informs the CSA of its intention to do so and receives the assent of the CSA (which will have contacted the complainant in this respect). The LSA contacts the controller and invites it to comply with the requests. The controller complies with the access request, however it does not intend to rectify the information held on the complainant on account of a payment claim that is pending against the complainant on the basis of such information. The LSA submits a draft decision to the CSA containing a short description of the case, the proposed settlement of the access request and the relevant terms; at the same time, the LSA informs the CSA that a separate case will be opened to investigate the rejection of the complainant's rectification request by the controller. In the absence of reasoned and relevant objections by the CSA, the LSA will adopt the decision on the amicable settlement of the access request and notify it to the controller whilst the CSA will inform the complainant thereof in pursuance of Article 60(7), second sentence, of the GDPR.

### 3.2.3 Cases under Article 56(2)

44. A derogation from the OSS rule is represented by the so-called "local case" situation under Article 56(2) GDPR. Reference can be made in this respect, as already pointed out<sup>16</sup>, to Recital 131 which mentions the "amicable settlement" in connection with cross-border "processing activities" having local impact.
45. Indeed, Recital 131 has to be taken also into account if the case has been found to be handled locally, i.e. by the CSA that has received the complaint, under Article 56(2). Underpinning the options that SAs have when it comes to case handling in such cases, Recital 131 serves as an interpretation aid. CSAs are expressly invited to seek amicable settlement ("should seek an amicable settlement with the controller") when there is a case with sole local as well as minor impacts. Thus, Recital 131 suggests that a CSA should preferably seek an amicable settlement in "local cases" (if at all feasible, again in the light of the conditions set out in paragraphs 11 and 12).
46. As already pointed out, since cooperation in the OSS context is aimed at reaching "consensus" and requires that "all relevant information" be exchanged between CSA and LSA, the LSA must be informed of the settlements achieved, if any, as the "systemic" features of the infringement or non-compliance underlying the complaint can only be assessed in full by the LSA.
47. The EDPB recalls, whilst the complainant may be satisfied with the settlement, in particular because access was granted in full, their data were rectified as requested, or erasure of their data took place, that settlement as reached by the CSA does not exhaust the remedies available to the LSA. Indeed, irrespective of whether an amicable settlement has been reached, the LSA has the option of initiating

<sup>16</sup> See paragraphs 23 and 24.

an official investigation (ex officio) in this case, whereupon the entire OSS procedure is then activated in accordance with Article 60 GDPR. The LSA may decide in all cases to investigate and take corrective measures, including fines, against that controller's main establishment in cases of repeated infringements or of non-compliance with data subjects' requests as communicated, *inter alia*, by other CSAs in similar circumstances.

48. In the context of an Article 56(2) procedure, the CSA should provide relevant information to the LSA as well as consider mutual assistance, and should put in place measures for effective cooperation, including information on the outcome of the settlement and/or of the results of the exercise of its full range of powers under Article 56(5) GDPR.

## 4 LEGAL CONSEQUENCES AND PRACTICAL RECOMMENDATIONS

### 4.1 Application of the principle of good administration to the amicable settlement procedure in the OSS context

49. The amicable settlement procedure in the context of the OSS as outlined above<sup>17</sup> should be read in light of the general principle of the right to good administration – and in line with the general principle of due process as recalled in Recital 129 and Article 58(4) GDPR: That is to say, the amicable settlement procedure, being applied by an SA empowered to deploy this type of administrative remedy, should respect the principle of good administration and due process in all cases.<sup>18</sup>
50. When it receives a complaint, the CSA, in the first step, has to clarify its specific role<sup>19</sup> according to Articles 55 and 56 GDPR. The importance of the “vetting” phase following the submission of a complaint to an SA should be emphasized in this respect<sup>20</sup>, regardless of the route or pathway that the particular case takes afterwards as the relevant elements shall be included in the file from an early date.
51. In the second step, the case in question must also be considered from the point of view of the parties involved, namely the data subject who lodged the complaint, the controller(s) and possible processor(s). Their relationship and the nature of the complaint will determine whether an amicable settlement can lead to a solution, namely the controller's compliance with the GDPR and satisfaction of the data subject. Last but not least, the outcome of such procedures for each SA and the legal consequences for the parties involved will have to be examined in more detail to assess whether a case is in the end suitable for an amicable settlement.

---

<sup>17</sup> See Part 3 “General legal analysis”.

<sup>18</sup> Which entails, as a minimum, the right of every person to be heard, before any individual measure which would affect him or her adversely is taken; the right of every person to have access to his or her file, while respecting the legitimate interests of confidentiality and of professional and business secrecy; the obligation of the administration to give reasons for its decisions.

<sup>19</sup> Lead or concerned Supervisory Authority ex Art. 56(1) GDPR.

<sup>20</sup> See WP244 rev. 01 and paragraph 50 of the EDPB Guidelines 02/2022 on the application of Article 60 GDPR.

52. If an amicable settlement is reached to the full satisfaction of all the parties concerned (objectified in the manner recommended in the preceding section) within the preliminary vetting process (aimed also, though not exclusively, to assess the applicability of Article 56(2) GDPR), the CSA where the complaint was lodged should not pass on the complaint to the assumed LSA (e.g., through an Article 56 IMI notification), as the object of the complaint is no longer present (cf. paragraph 24).
53. However, the receiving SA should communicate the case and the outcome to the LSA at an appropriate time, for instance on a quarterly basis (e.g., through the Voluntary Mutual Assistance procedure). This is meant to enable the LSA to fully discharge its role as “sole interlocutor” (for all intents and purposes) of the controller/processor at issue (see Article 56(6) GDPR). If the CSA, in the course of the preliminary vetting phase, does not manage to achieve an amicable settlement at all or only a settlement regarding parts of the complaint lodged with it and notified to the LSA, this information regarding the unsuccessful settlement should in any case be passed on to the LSA being unquestionably “relevant information” in the sense of Article 60(1) GDPR.

#### [4.2 The cooperation procedure following an amicable settlement achieved by the LSA](#)

54. The amicable settlement procedure should respect the conditions recalled, in particular, in the GDPR (Article 60, Recitals 129 and 143) as it has to result in a decision by the competent SA (the LSA, in an OSS context), after this decision has been found within the cooperation procedure. Reference should be made in this regard to the analysis on the rationale and contents of the draft decision to be submitted by the LSA, as contained in the Article 60 Guidance<sup>21</sup> (see paragraphs 109-111 in particular).
55. Accordingly, the amicable settlement achieved in the OSS context regarding a complaint requires a decision by the LSA in accordance with Article 60(3) GDPR as this is an obligation imposed on the LSA in all cross-border processing cases. It will be a “sui generis” decision finding that the complaint has been settled by the LSA with the mutual satisfaction of the parties involved (particularly data subject, data controller).
56. An amicable settlement could be considered as the use of some of the SA’s powers which do not imply the corrective powers referred to in Article 58(2). Nevertheless, as stated above (see paragraphs 15 and 43), depending on national law the LSA might not be prevented from using such powers even in amicable settlement cases.
57. Accordingly, the draft decision should include the following information:
  - o that the complaint was settled amicably, in whole or in part,
  - o the reasons underlying the decision to seek an amicable settlement in the specific case,
  - o the scope of the amicable settlement in light of the overall issues addressed in the complaint,
  - o that the handling of the specific complaint will be terminated.

---

<sup>21</sup> EDPB Guidelines 02/2022 on the application of Article 60 GDPR.

58. The draft decision may also indicate that the alleged infringement was remedied and how this was done.
59. Furthermore, if applicable, the draft decision and/or the relevant information given to the CSA(s) may include information about any intended corrective measures, which may especially be the case when the amicable settlement was only reached in part.
60. In all cases the LSA should inform the data subject of the consequences of the amicable settlement in a comprehensive way, in particular that the settlement will result in termination of the handling of the complaint. This information on the scope of the amicable settlement and its consequences must be conveyed by way of the CSA, which is the key interlocutor for the data subject in the whole process. To that end, the informal procedures developed as part of the IMI-mechanisms can be used, in particular an Art. 60 “Informal Consultation” procedure or an Art. 61 “Voluntary Mutual Assistance” procedure can be launched by the LSA in order to convey the proposed outcome of the case and obtain views from the CSAs involved before moving to the formal circulation of a draft decision.
61. As in the majority of Member States an amicable settlement applies only to the parties to the complaint (data subject, controller/processor, and, if applicable, also SA), and the controller or processor commits to a remedy of the infringement and the implementation of measures to ensure compliance with the GDPR, the scope of the settlement may only cover parts of the complaint. In this case, the remaining parts are subject to the LSA’s further investigation and decision.

#### 4.3 Amicable settlement in Article 56(2) cases

62. Regarding amicable settlements in cases where a CSA handles a complaint under Article 56(2) (i.e., as a local case)<sup>22</sup>, the SA should be mindful of the need for transparency and consistency that underlies the whole OSS system, and should therefore take care to provide regular (if aggregate) information to other SAs regarding such cases.
63. In particular, the CSA should inform the LSA about the settlement (if any) as outcome of the local case, through the IMI system. Since the settlement may only cover part of the complaint handled locally by the CSA, the CSA may take additional (including corrective) measures with regard to such remaining parts that have not been settled to the satisfaction of the parties in the manner described above. The CSA must inform the complainant according to Article 77(2) that the remaining parts of the complaint will be processed.

---

<sup>22</sup> Under Article 56(5) GDPR, the CSA “shall handle [the case] according to Articles 61 and 62”, i.e. by exercising its full powers (also pursuant to Article 56(1) GDPR).

## ANNEX 1: RELEVANT STEPS WHEN HANDLING A CASE VIA AMICABLE SETTLEMENT

64. The following check list intends to describe the concrete steps when handling cases that may be suitable for an amicable settlement. The check list is therefore not to be understood in the sense of a 'yes/no' chart showing different consequences, but rather as an overview of the concrete different stages in the proceeding as well as of the relevant steps to take as a best practice. While section 1) is to recall the basic facts of the case, not ticking one of the boxes in sections 2) to 5) could lead to the authority having to take further steps.

### **Checklist: Steps in handling a case via amicable settlement**

#### **1) Background of the case**

- ) How has the proceeding been started?
  - Complaint
  - Media reports, ex officio investigations, etc.
  - Hints from third persons concerned
- ) What is the nature of the case?
  - Local case (Article 56(2) and Recital 131 GDPR)
  - Cross-border processing case
- ) Case suitable for amicable settlement, because (cf. paragraph 14)
  - o limited amount of data subjects affected
  - o systemic failure not recognisable
  - o incidental or accidental data protection violation
  - o limited number of personal data
  - o effects of the violation not of serious duration/nature
  - o likelihood of further violations in the future
  - o no/little societal significance/public interest
  - o ...

#### **2) Early Cooperation with other SAs (where applicable)**

- ) Effects of any action already taken in the procedure  
(e.g. for the LSA, if applicable: Has the CSA already attempted an amicable settlement in the preliminary vetting?)  
.....

- ) LSA consulted (where applicable)
  - Translated Version of complaint
  - Previous communication between data subject and controller
  - Other important information

- ✓ Other CSA(s) consulted
- Translated Version of complaint
- Other important information

**3) Consultation of all concerned parties at an early stage**

- ✓ Data subject 
  - General information according to Article 77(2) GDPR provided
  - General interest in an amicable resolution
  - No other reasons for specific treatment of the case
  - This information has been shared with the involved CSA and, where applicable, the LSA
- ✓ Controller/processor 
  - An official hearing has taken place
  - The controller/processor is willing to establish compliance to legal requirements
  - There is a chance to gain compliance within an appropriate time frame
  - This information has been shared with the involved CSA and, where applicable, the LSA (e.g. via informal consultation)
- ✓ Third party (where applicable) 
  - No rights of a third party affected
  - There are no rights of third parties precluding an agreement (e.g. because granting the complainant's request for access impacts the data protection rights of a third party)

**4) Has an amicable settlement been reached?**

- ✓ Satisfaction of the data subject demonstrated 
  - The infringement for which you have been notified is remedied
  - No objections from the data subject
  - The data subject came back to you in an appropriate time frame
- ✓ The controller/processor provided proof of compliance
- ✓ Where applicable: The LSA/CSA was provided with this information

**5) Does the final decision comply with Article 60 GDPR (in OSS cases)?**

- ✓ The decision contains all relevant information (cf. paragraphs 57 et seq.)
- ✓ The (if applicable: revised) draft decision has been circulated via IMI 
  - The draft decision has been sent

- There have been no reasoned and relevant objections
- There have been reasoned and relevant objections, but all of them could be overcome

) The final decision has been circulated via IMI

- The controller/processor has been notified of the decision
- The data subject has been informed of the decision

## ANNEX 2: COUNTRIES WHERE AMICABLE SETTLEMENTS ARE NOT POSSIBLE IN ACCORDANCE WITH THE NATIONAL LEGISLATION

65. The following countries have indicated that amicable settlements are not possible in accordance with their national legislation:

- Cyprus
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Greece
- Malta
- Poland
- Portugal
- Slovakia
- Slovenia
- Spain
- Sweden

# Guidelines



**Guidelines 8/2022 on identifying a controller or processor's  
lead supervisory authority**

**Version 2.1**

**Adopted on 28 March 2023**

## Version history

Version 1.0	10 October 2022	Adoption of the Guidelines (updated version of the previous guidelines WP244 rev.01 adopted by the Working Party 29 and endorsed by the EDPB on 25 May 2018) for a targeted public consultation.
Version 2.0	28 March 2023	Adoption of the Guidelines after public consultation
Version 2.1	28 September 2023	Minor correction made to footnote 12 on p. 10.

## Table of contents

0	Preface.....	4
1	Identifying a lead supervisory authority: the key concepts .....	5
1.1	‘Cross-border processing of personal data’.....	5
1.1.1	‘Substantially affects’.....	5
1.2	Lead supervisory authority .....	6
1.3	Main establishment.....	6
2	Steps to identify the lead supervisory authority .....	7
2.1	Identify the ‘main establishment’ for controllers.....	7
2.1.1	Criteria for identifying a controller’s main establishment in cases where it is not the place of its central administration in the EEA.....	8
2.1.2	Groups of undertakings.....	9
2.1.3	Joint controllers .....	9
2.2	Borderline cases.....	10
2.3	Processor .....	11
3	Other relevant issues.....	11
3.1	The role of the ‘supervisory authority concerned’ .....	11
3.2	Local processing.....	12
3.3	Companies not established within the EU .....	12
	ANNEX - Questions to guide the identification of the lead supervisory authority .....	13
1	Is the controller or processor carrying out the cross-border processing of personal data? ....	13
2	How to identify the ‘lead supervisory authority’ .....	13
3	Are there any ‘concerned supervisory authorities’? .....	14

# The European Data Protection Board

Having regard to Article 70(1)(e) and (l) 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<sup>1</sup>,

Having regard to Article 12 and Article 22 of its Rules of Procedure,

Having regard to the Article 29 Working Party Guidelines for identifying a controller or processor’s lead supervisory authority, WP244 rev.01,

Having regard to the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR,

## HAS ADOPTED THE FOLLOWING GUIDELINES

### 0 PREFACE

1. On 5 April 2017, the Article 29 Working Party adopted its Guidelines for identifying a controller or processor’s lead supervisory authority (WP244 rev.01)<sup>2</sup>, which were endorsed by the European Data Protection Board (hereinafter “EDPB”) at its first Plenary meeting<sup>3</sup>. This document is a slightly updated version of those guidelines. Any reference to the WP29 Guidelines for identifying a controller or processor’s lead supervisory authority (WP244 rev.01) should, from now on, be interpreted as a reference to these EDPB guidelines.
2. The EDPB has noticed that there was a need for further clarifications, specifically regarding the notion of main establishment in the context of joint controllership and taking into account the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR<sup>4</sup>.
3. The paragraph concerning this matter has been revised and updated, while the rest of the document was left unchanged, except for editorial changes. The revision concerns, more specifically, Section 2.1.3 on joint controllers.

---

<sup>1</sup> References to “Member States” made throughout this document should be understood as references to “EEA Member States”.

<sup>2</sup> Available at [http://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=611235](http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611235).

<sup>3</sup> See [https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb\\_en](https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en).

<sup>4</sup> See Guidelines 07/2020 on the concepts of controller and processor in the GDPR, version 2.0 adopted on 7 July 2021, paragraphs 161, 162 and 166, available at [https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr\\_en](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en)

# 1 IDENTIFYING A LEAD SUPERVISORY AUTHORITY: THE KEY CONCEPTS

## 1.1 ‘Cross-border processing of personal data’

4. Identifying a lead supervisory authority is only relevant where a controller or processor is carrying out the cross-border processing of personal data. Article 4(23) GDPR defines ‘cross-border processing’ as either the:
    - *processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or the*
    - *processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.*
  5. This means that where an organisation has establishments in France and Romania, for example, and the processing of personal data takes place in the context of their activities, then this will constitute cross-border processing.
  6. Alternatively, the organisation may only carry out processing activity in the context of its establishment in France. However, if the activity substantially affects – or is likely to substantially affect – data subjects in France and Romania then this will also constitute cross-border processing.
- 1.1.1 ‘Substantially affects’
7. The GDPR does not define ‘substantially’ or ‘affects’. The intention of the wording was to ensure that not all processing activity, with *any* effect and that takes place within the context of a single establishment, falls within the definition of ‘cross-border processing’.
  8. The most relevant ordinary English meanings of ‘substantial’ include: ‘of ample or considerable amount or size; sizeable, fairly large’, or ‘having solid worth or value, of real significance; solid; weighty, important’<sup>5</sup>.
  9. The most relevant meaning of the verb ‘affect’ is ‘to influence’ or ‘to make a material impression on’. The related noun -‘effect’- means, amongst other things, ‘a result’ or ‘a consequence’<sup>6</sup>. This suggests that for data processing to affect someone it must have some form of impact on them. Processing that does not have a substantial effect on individuals does not fall within the second part of the definition of ‘cross-border processing’. However, it would fall within the first part of the definition where the processing of personal data takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union, where the controller or processor is established in more than one Member State.
  10. Processing can be brought within the second part of the definition if there is the likelihood of a substantial effect, not just an actual substantial effect. Note that ‘likely to’ does not mean that there is a remote possibility of a substantial effect. The substantial effect must be more likely than not. On the other hand, it also means that individuals do not have to be actually affected: the likelihood of a substantial effect is sufficient to bring the processing within the definition of ‘cross-border processing’.

---

<sup>5</sup> Oxford English Dictionary.

<sup>6</sup> Oxford English Dictionary.

11. The fact that a data processing operation may involve the processing of a number – even a large number – of individuals' personal data, in a number of Member States, does not necessarily mean that the processing has, or is likely to have, a substantial effect. Processing that does not have a substantial effect does not constitute cross-border processing for the purposes of the second part of the definition, regardless of how many individuals it affects.
12. Supervisory Authorities will interpret 'substantially affects' on a case by case basis. We will take into account the context of the processing, the type of data, the purpose of the processing and factors such as whether the processing:
  - causes, or is likely to cause, damage, loss or distress to individuals;
  - has, or is likely to have, an actual effect in terms of limiting rights or denying an opportunity;
  - affects, or is likely to affect individuals' health, well-being or peace of mind;
  - affects, or is likely to affect, individuals' financial or economic status or circumstances;
  - leaves individuals open to discrimination or unfair treatment;
  - involves the analysis of the special categories of personal or other intrusive data, particularly the personal data of children;
  - causes, or is likely to cause individuals to change their behaviour in a significant way;
  - has unlikely, unanticipated or unwanted consequences for individuals;
  - creates embarrassment or other negative outcomes, including reputational damage; or
  - involves the processing of a wide range of personal data.

13. Ultimately, the test of 'substantial effect' is intended to ensure that supervisory authorities are only required to co-operate formally through the GDPR's consistency mechanism "*where a supervisory authority intends to adopt a measure intended to produce legal effects as regards processing operations which substantially affect a significant number of data subjects in several Member States*"<sup>7</sup>.

## 1.2 Lead supervisory authority

14. Put simply, a 'lead supervisory authority' is the authority with the primary responsibility for dealing with a cross-border data processing activity, for example when a data subject makes a complaint about the processing of his or her personal data.
15. The lead supervisory authority will coordinate any investigation, involving other 'concerned' supervisory authorities.
16. Identifying the lead supervisory authority depends on determining the location of the controller's 'main establishment' or 'single establishment' in the EU. Article 56 GDPR says that:
  - *the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the [cooperation] procedure provided in Article 60.*

## 1.3 Main establishment

17. Article 4(16) GDPR states that 'main establishment' means:

---

<sup>7</sup> See Recital 135 GDPR.

- *as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;*
- *as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;*

## 2 STEPS TO IDENTIFY THE LEAD SUPERVISORY AUTHORITY

### 2.1 Identify the ‘main establishment’ for controllers

18. In order to establish where the main establishment is, it is firstly necessary to identify the central administration of the controller in the EEA, if any. The approach implied in the GDPR is that the central administration in the EU is the place where decisions about the purposes and means of the processing of personal data are taken, and this place has the power to have such decisions implemented.
19. The essence of the lead supervisory authority principle in the GDPR is that the supervision of cross-border processing should be led by only one supervisory authority in the EU. In cases where decisions relating to different cross-border processing activities are taken within the EU central administration, there will be a single lead supervisory authority for the various data processing activities carried out by the multinational company. However, there may be cases where an establishment other than the place of central administration makes autonomous decisions concerning the purposes and means of a specific processing activity. This means that there can be situations where more than one lead supervisory authority can be identified, i.e. in cases where a multinational company decides to have separate decision-making centres, in different countries, for different processing activities.
20. It is worth recalling, that where a multinational company centralises all the decisions relating to the purposes and means of processing activities in one of its establishments in the EEA (and that establishment has the power to implement such decisions), only one lead supervisory authority will be identified for the multinational.
21. In these situations, it will be essential for companies to identify precisely where the decisions on purpose and means of processing are taken. Correct identification of the main establishment is in the interests of controllers and processors because it provides clarity in terms of which supervisory authority they have to deal with in respect of their various compliance duties under the GDPR. These may include, where relevant, designating a data protection officer or consulting for a risky processing activity that the controller cannot mitigate by reasonable means. The relevant provisions of the GDPR are intended to make these compliance tasks manageable.
22. The examples below illustrate this:

**Example 1:** A food retailer has its headquarters (i.e., its ‘place of central administration’) in Rotterdam, Netherlands. It has establishments in various other EEA countries, which are in contact with individuals there. All establishments make use of the same software to process consumers’ personal data for marketing purposes. All the decisions about the purposes and means of the processing of consumers’ personal data for marketing purposes are taken within its Rotterdam headquarters. This means that

the company's lead supervisory authority for this cross-border processing activity is the Dutch supervisory authority.

Example 2: A bank has its corporate headquarters in Frankfurt, and all<sup>8</sup> its banking processing activities are organised from there, but its insurance department is located in Vienna. If the establishment in Vienna has the power to decide on all insurance data processing activities and to implement these decisions for the whole EEA, then, as foreseen in Article 4(16) GDPR, the Austrian supervisory authority would be the lead supervisory authority in respect of the cross-border processing of personal data for insurance purposes, and the competent German supervisory authority (i.e., the Hessen supervisory authority) would supervise the processing of personal data for banking purposes, wherever the clients are located<sup>9</sup>.

#### 2.1.1 Criteria for identifying a controller's main establishment in cases where it is not the place of its central administration in the EEA

23. Recital 36 GDPR is useful in clarifying the main factor that shall be used to determine a controller's main establishment if the criterion of the central administration does not apply. This involves identifying where the effective and real exercise of management activities, that determine the main decisions as to the purposes and means of processing through stable arrangements, takes place. Recital 36 GDPR also clarifies that "*the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute a main establishment and are therefore not determining criteria for a main establishment*".
24. The controller itself identifies where its main establishment is and therefore which supervisory authority is its lead supervisory authority. However, this can be challenged by the respective supervisory authority concerned afterwards.
25. The factors below are useful for determining the location of a controller's main establishment, according to the terms of the GDPR, in cases where it is not the location of its central administration in the EEA.
  - Where are decisions about the purposes and means of the processing given final 'sign off'?
  - Where are decisions about business activities that involve data processing made?
  - Where does the power to have decisions implemented effectively lie?
  - Where is the Director (or Directors) with overall management responsibility for the cross-border processing located?
  - Where is the controller or processor registered as a company, if in a single territory?
26. Note that this is not an exhaustive list. Other factors may be relevant depending on the controller or processing activity in question. If a supervisory authority has reasons to doubt that the establishment

---

<sup>8</sup> In the context of processing personal data for banking purposes, the EDPB recognises that there are many different purposes pursued by these processing activities. However, to simplify matters, the EDPB addresses all of them as a single purpose. The same is true of processing done for insurance purposes.

<sup>9</sup> It should be recalled also that the GDPR provides for the possibility of local oversight in specific cases. See Recital 127: "*Each supervisory authority not acting as the lead supervisory authority should be competent to handle local cases where the controller or processor is established in more than one Member State, but the subject matter of the specific processing concerns only processing carried out in a single Member State and involves only data subjects in that single Member State*, for example, where the subject matter concerns the processing of employees' personal data in the specific employment context of a Member State."

This principle means that the supervision of HR data connected to the local employment context could fall on several supervisory authorities.

identified by the controller is in reality the main establishment for the purposes of the GDPR, it can – of course – require the controller to provide the additional information necessary for it to prove where its main establishment is located.

### 2.1.2 Groups of undertakings

27. Where processing is carried out by a group of undertakings that has its headquarters in the EEA, the establishment of the undertaking with overall control is presumed to be the decision-making centre relating to the processing of personal data, and will therefore be considered to be the main establishment for the group, except where decisions about the purposes and means of processing are taken by another establishment. The parent, or operational headquarters of the group of undertakings in the EEA, is likely to be the main establishment, because that would be the place of its central administration.
28. The reference in the definition to the place of a controller's central administration works well for organisations that have a centralised decision-making headquarters and branch-type structure. In such cases, it is clear that the power to make decisions about cross-border processing, and to have them carried out, lies within the company's headquarters. In such cases, determining the location of the main establishment - and therefore which supervisory authority is the lead supervisory authority - is straightforward. However, the decision system of group of companies could be more complex, giving independent making powers relating to cross-border processing to different establishments. The criteria set out above should help groups of undertakings to identify their main establishment.

### 2.1.3 Joint controllers

29. The GDPR does not specifically deal with the issue of designating a lead supervisory authority where two or more controllers established in the EEA jointly determine the purposes and means of processing - i.e. joint controllers. Article 26(1) and Recital 79 GDPR make it clear that in joint controllership situations, the controllers shall in a transparent manner determine their respective responsibilities for compliance with their obligations under the GDPR.
30. As recalled by the EDPB in its Guidelines on the concept of controller and processor<sup>10</sup>, joint controllers need to set "who does what" by deciding between themselves who will have to carry out which tasks, in order to make sure that the processing complies with the applicable obligations under the GDPR in relation to the joint processing at stake.
31. The compliance measures and related obligations joint controllers should consider when determining their respective responsibilities, in addition to those specifically referred in Article 26(1) GDPR, include, amongst others, the organisation of contact with data subjects and supervisory authorities.
32. It should be recalled that supervisory authorities are not bound by the terms of such arrangement, neither on the issue of the qualification of the parties as joint controllers nor on the designated contact point<sup>11</sup>.
33. Moreover, the decision-making power of joint controllers does not comprise the determination of the competent supervisory authority according to Articles 55 and 56 GDPR, or the ability of these supervisory authorities to exercise their tasks and powers as described in Articles 57 and 58 GDPR.

---

<sup>10</sup> See Guidelines 07/2020 on the concepts of controller and processor in the GDPR, paragraphs 161, 162 and 166.

<sup>11</sup> See Guidelines 07/2020 on the concepts of controller and processor in the GDPR, paragraph 191.

34. The notion of main establishment is linked by virtue of the GDPR to a single controller and cannot be extended to a joint controllership situation. This is without prejudice to the possibility for each joint controller to have its own main establishment. In other words, the main establishment of a controller cannot be considered as the main establishment of the joint controllers for the processing carried out under their joint control. Therefore, joint controllers cannot designate (among the establishments where decisions on the purposes and means of the processing are taken) a common main establishment for both joint controllers.

## 2.2 Borderline cases

35. There will be borderline and complex situations where it is difficult to identify the main establishment or to determine where decisions about data processing are taken. This might be the case where there is cross-border processing activity and the controller is established in several Member States, but there is no central administration in the EEA and none of the EEA establishments are taking decisions about the processing (i.e. decisions are taken exclusively outside of the EEA).
36. In the case above, the company carrying out cross-border processing may be keen to be regulated by a lead supervisory authority to benefit from the one-stop-shop principle. However, the GDPR does not provide a solution for situations like this. In these circumstances, the company should designate the establishment that has the authority to implement decisions about the processing activity and to take liability for the processing, including having sufficient assets, as its main establishment. If the company does not designate a main establishment in this way, it will not be possible to designate a lead supervisory authority. Supervisory authorities will always be able to investigate further where this is appropriate.
37. The GDPR does not permit ‘forum shopping’. If a company claims to have its main establishment in one Member State, but no effective and real exercise of management activity or decision-making over the processing of personal data takes place there, the relevant supervisory authorities (or ultimately the EDPB<sup>12</sup>) will decide which supervisory authority is the ‘lead’, using objective criteria and looking at the evidence. The process of determining where the main establishment is may require active inquiry and co-operation by the supervisory authorities. Conclusions cannot be based solely on statements by the organisation under review. The burden of proof ultimately falls on controllers and processors to demonstrate to the relevant supervisory authorities where the relevant processing decisions are taken and where there is the power to implement such decisions. Effective records of data processing activity would help both organisations and supervisory authorities to determine the lead supervisory authority. The lead supervisory authority, or concerned supervisory authorities, can rebut the controller’s analysis based on an objective examination of the relevant facts, requesting further information where required.
38. In some cases, the relevant supervisory authorities will ask the controller to provide clear evidence, in line with any EDPB guidelines, of where its main establishment is, or where decisions about a particular data processing activity are taken. This evidence will be given due weight and the supervisory authorities involved will co-operate to decide which one of them will take the lead in investigations. Such cases will only be referred to the EDPB for a decision under Article 65(1)(b) GDPR where supervisory authorities have conflicting views in terms of identifying the lead supervisory authority. However, in most cases, the EDPB expects that the relevant supervisory authorities will be able to agree a mutually satisfactory course of action.

---

<sup>12</sup> See paragraph 38 below.

## 2.3 Processor

39. The GDPR also offers the one-stop-shop system for the benefit of processors that are subject to GDPR and have establishments in more than one Member State.
40. Article 4(16)(b) GDPR states that the processor's main establishment will be the place of the central administration of the processor in the EU or, if there is no central administration in the EU, the establishment in the EU where the main processing (processor) activities take place.
41. However, according to Recital 36 GDPR, in cases involving both a controller and a processor, the competent lead supervisory authority should be the lead supervisory authority for the controller. In this situation, the supervisory authority of the processor will be a 'supervisory authority concerned' and should participate in the cooperation procedure. This rule will only apply where the controller is established in the EEA. In cases where controllers are subject to the GDPR on the basis of its Article 3(2), they will not be subject to the one-stop-shop mechanism. A processor - for example, a large cloud-service provider - may provide services to multiple controllers located in different Member States. In such cases, the lead supervisory authority will be the supervisory authority that is competent to act as lead for the controller. In effect, this means a processor may have to deal with multiple supervisory authorities.

## 3 OTHER RELEVANT ISSUES

### 3.1 The role of the 'supervisory authority concerned'

42. GDPR Article 4(22) says that the:

*'supervisory authority concerned' means a supervisory authority which is concerned by the processing of personal data because: (a) the controller or processor is established on the territory of the Member State of that supervisory authority; (b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or (c) a complaint has been lodged with that supervisory authority.'*

43. The concept of a concerned supervisory authority is meant to ensure that the 'lead supervisory authority' model does not prevent other supervisory authorities having a say in how a matter is dealt with when, for example, individuals residing outside the lead supervisory authority's jurisdiction are substantially affected by a data processing activity. In terms of factor (a) above, the same considerations as for identifying a lead supervisory authority apply. Note that in (b) the data subject must merely reside in the Member State in question; they do not have to be a citizen of that State. It will generally be easy in (c) to determine - as a matter of fact - whether a particular supervisory authority has received a complaint.
44. Article 56, paragraphs (2) and (5) GDPR provide for a concerned supervisory authority to take a role in dealing with a case without being the lead supervisory authority. When a lead supervisory authority decides not to handle a case, the concerned supervisory authority that informed the lead supervisory authority shall handle it. This is in accordance with the procedures in Article 61 (Mutual assistance) and Article 62 (Joint operations of supervisory authorities) GDPR. This might be the case where a marketing company with its main establishment in Paris launches a product that only affects data subjects residing in Portugal. In such a case, the French and Portuguese supervisory authorities might agree that it is appropriate for the Portuguese supervisory authority to take the lead in dealing with the matter. Supervisory authorities may request that controllers provide input in terms of clarifying their corporate arrangements. Given that the processing activity has a purely local effect - i.e. on

individuals in Portugal - the French and Portuguese supervisory authorities have the discretion to decide which supervisory authority should deal with the matter - in accordance with Recital 127 GDPR.

45. The GDPR requires lead and concerned supervisory authorities to co-operate, with due respect for each other's views, to ensure a matter is investigated and resolved to each authority's satisfaction - and with an effective remedy for data subjects. Supervisory authorities should endeavour to reach a mutually acceptable course of action. The formal consistency mechanism should only be invoked where co-operation does not reach a mutually acceptable outcome.
46. The mutual acceptance of decisions can apply to substantive conclusions, but also to the course of action decided upon, including enforcement activity (e.g. full investigation or an investigation with limited scope). It can also apply to a decision not to handle a case in accordance with the GDPR, for example because of a formal policy of prioritisation, or because there are other concerned authorities as described above.
47. The development of consensus and good will between supervisory authorities is essential to the success of the GDPR's cooperation and consistency procedures.

### 3.2 Local processing

48. Local data processing activity does not fall within the GDPR's cooperation and consistency provisions. Supervisory authorities will respect each other's competence to deal with local data processing activity on a local basis. Processing carried out by public authorities will always be dealt with on a 'local' basis, too.

### 3.3 Companies not established within the EEA

49. The GDPR's cooperation and consistency mechanisms only apply to controllers with an establishment, or establishments, within the EEA. If a company does not have an establishment in the EEA, the mere presence of a representative in a Member State does not trigger the one-stop-shop principle. This means that controllers without any establishment in the EEA must deal with local supervisory authorities in every Member State they are active in, through their local representative.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

## ANNEX - QUESTIONS TO GUIDE THE IDENTIFICATION OF THE LEAD SUPERVISORY AUTHORITY

1 Is the controller or processor carrying out the cross-border processing of personal data?

a. Yes, if:

- The controller or processor is established in more than one Member State, and
- The processing of personal data takes place in the context of the activities of establishments in more than one Member State.

➤ In this case, go to section 2.

b. Yes, if:

- The processing of personal data takes place in the context of the activities of a controller or processor's single establishment in the EEA, but:
- Substantially affects or is likely to substantially affect individuals in more than one Member State.

➤ In this case, the lead supervisory authority is the authority for the controller or processor's single establishment in a single Member State. This is - by logic - the controller or processor's main establishment because it is its only establishment.

2 How to identify the 'lead supervisory authority'

a. In a case involving only a controller:

- Identify the controller's place of central administration in the EEA;
- The supervisory authority of the country where the place of central administration is located is the controller's lead supervisory authority.

However:

- If decisions on the purposes and means of the processing are taken in another establishment in the EEA, and that establishment has the power to implement those decisions, then the lead supervisory authority is the one located in the country where this establishment is.

b. In a case involving a controller and a processor:

- Check if the controller is established in the EEA and subject to the one-stop-shop system If so,
- Identify the lead supervisory authority of the controller. This authority will also be the lead supervisory authority for the processor.
- The (non-lead) supervisory authority competent for the processor will be a 'concerned supervisory authority' - see section 3 below.

c. In a case involving only a processor:

- Identify the processor's place of central administration in the EEA;

- ii. If the processor has no central administration in the EEA, identify the establishment in the EEA where the main processing activities of the processor take place.
- d. In a case involving joint controllers:
  - i. Check if the joint controllers are established in the EEA.
  - ii. Identify the place of central administration in the EEA for each joint controller respectively (where applicable);
  - iii. The supervisory authority of the country where the place of central administration is located is the lead supervisory authority of the respective joint controller.

### 3 Are there any 'concerned supervisory authorities'?

An authority is a 'concerned authority':

- When the controller or processor has an establishment on its territory, or;
- When data subjects on its territory are substantially affected or likely to be substantially affected by the processing, or;
- When a complaint is received by a particular supervisory authority.

# Guidelines



**Guidelines 9/2022 on personal data breach notification  
under GDPR**

**Version 2.0**

**Adopted 28 March 2023**

## Version history

Version 1.0	10 October 2022	Adoption of the Guidelines (updated version of the previous guidelines WP250 (rev.01) adopted by the Working Party 29 and endorsed by the EDPB on 25 May 2018) for a targeted public consultation.
Version 2.0	28 March 2023	Adoption of the Guidelines following the targeted public consultation on the subject of data breach notification for controllers not established in the EEA.

## TABLE OF CONTENTS

<b>0</b>	<b>PREFACE .....</b>	<b>5</b>
<b>INTRODUCTION .....</b>		<b>5</b>
<b>I.</b>	<b>PERSONAL DATA BREACH NOTIFICATION UNDER THE GDPR.....</b>	<b>7</b>
A.	Basic security considerations .....	7
B.	What is a personal data breach?.....	7
	1. <i>Definition</i> .....	7
	2. <i>Types of personal data breaches</i> .....	8
	3. <i>The possible consequences of a personal data breach</i> .....	9
<b>II.</b>	<b>ARTICLE 33 - NOTIFICATION TO THE SUPERVISORY AUTHORITY .....</b>	<b>10</b>
A.	When to notify.....	10
	1. <i>Article 33 requirements</i> .....	10
	2. <i>When does a controller become “aware”?</i> .....	11
	3. <i>Joint controllers</i> .....	13
	4. <i>Processor obligations</i> .....	13
B.	Providing information to the supervisory authority.....	14
	1. <i>Information to be provided</i> .....	14
	2. <i>Notification in phases</i> .....	15
	3. <i>Delayed notifications</i> .....	16
C.	Cross-border breaches and breaches at non-EU establishments.....	17
	1. <i>Cross-border breaches</i> .....	17
	2. <i>Breaches at non-EU establishments</i> .....	17
D.	Conditions where notification is not required .....	18
<b>III.</b>	<b>ARTICLE 34 – COMMUNICATION TO THE DATA SUBJECT.....</b>	<b>20</b>
A.	Informing individuals .....	20
B.	Information to be provided .....	20
C.	Contacting individuals.....	21
D.	Conditions where communication is not required .....	22
<b>IV.</b>	<b>ASSESSING RISK AND HIGH RISK.....</b>	<b>23</b>
A.	Risk as a trigger for notification .....	23
B.	Factors to consider when assessing risk.....	23
<b>V.</b>	<b>ACCOUNTABILITY AND RECORD KEEPING .....</b>	<b>26</b>
A.	Documenting breaches.....	26
B.	Role of the Data Protection Officer.....	27
<b>VI.</b>	<b>NOTIFICATION OBLIGATIONS UNDER OTHER LEGAL INSTRUMENTS .....</b>	<b>28</b>

**VII. ANNEX .....****30**

A. Flowchart showing notification requirements.....	30
B. Examples of personal data breaches and who to notify .....	31

# The European Data Protection Board

Having regard to Article 70(1)(e) and (l) 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<sup>1</sup>,

Having regard to Article 12 and Article 22 of its Rules of Procedure,

Having regard to the Article 29 Working Party Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01,

## HAS ADOPTED THE FOLLOWING GUIDELINES

### 0 PREFACE

1. On 3 October 2017, the Working Party 29 (hereinafter “WP29”) adopted its Guidelines on Personal data breach notification under Regulation 2016/679 (WP250 rev.01)<sup>2</sup>, which were endorsed by the European Data Protection Board (hereinafter “EDPB”) at its first Plenary meeting<sup>3</sup>. This document is a slightly updated version of those guidelines. Any reference to the WP29 Guidelines on Personal data breach notification under Regulation 2016/679 (WP250 rev.01) should, from now on, be interpreted as a reference to these EDPB Guidelines 9/2022.
2. The EDPB noticed that there was a need to clarify the notification requirements concerning the personal data breaches at non-EU establishments. The paragraph concerning this matter has been revised and updated, while the rest of the document was left unchanged, except for editorial changes. The revision concerns, more specifically, paragraph 73 in Section II.C.2 of this document.

### INTRODUCTION

3. The GDPR introduced the requirement for a personal data breach (henceforth “breach”) to be notified to the competent national supervisory authority<sup>4</sup> (or in the case of a cross-border breach, to the lead authority) and, in certain cases, to communicate the breach to the individuals whose personal data have been affected by the breach.
4. Obligations to notify in cases of breaches existed for certain organisations, such as providers of publicly-available electronic communications services (as specified in Directive 2009/136/EC and Regulation (EU) No 611/2013)<sup>5</sup>. There were also some Member States that already had their own

---

<sup>1</sup> References to “Member States” made throughout this document should be understood as references to “EEA Member States”.

<sup>2</sup> WP29 Guidelines on Personal data breach notification under Regulation 2016/679 (WP250 rev.01) (last revised and updated on 6 February 2018), available at <https://ec.europa.eu/newsroom/article29/items/612052>.

<sup>3</sup> See [https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb\\_en](https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en).

<sup>4</sup> See Article 4(21) GDPR.

<sup>5</sup> See <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32009L0136> and <http://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A32013R0611>

national breach notification obligation. This might include the obligation to notify breaches involving categories of controllers in addition to providers of publicly available electronic communication services (for example in Germany and Italy), or an obligation to report all breaches involving personal data (such as in the Netherlands). Other Member States might have had relevant Codes of Practice (for example, in Ireland<sup>6</sup>). Whilst a number of EU data protection authorities encouraged controllers to report breaches, the Data Protection Directive 95/46/EC<sup>7</sup>, which the GDPR replaced, did not contain a specific breach notification obligation and therefore such a requirement was new for many organisations. The GDPR makes notification mandatory for all controllers unless a breach is unlikely to result in a risk to the rights and freedoms of individuals<sup>8</sup>. Processors also have an important role to play and they must notify any breach to their controller<sup>9</sup>.

5. The EDPB considers that the notification requirement has a number of benefits. When notifying the supervisory authority, controllers can obtain advice on whether the affected individuals need to be informed. Indeed, the supervisory authority may order the controller to inform those individuals about the breach<sup>10</sup>. Communicating a breach to individuals allows the controller to provide information on the risks presented as a result of the breach and the steps those individuals can take to protect themselves from its potential consequences. The focus of any breach response plan should be on protecting individuals and their personal data. Consequently, breach notification should be seen as a tool enhancing compliance in relation to the protection of personal data. At the same time, it should be noted that failure to report a breach to either an individual or a supervisory authority may mean that under Article 83 GDPR a possible sanction is applicable to the controller.
6. Controllers and processors are therefore encouraged to plan in advance and put in place processes to be able to detect and promptly contain a breach, to assess the risk to individuals<sup>11</sup>, and then to determine whether it is necessary to notify the competent supervisory authority, and to communicate the breach to the individuals concerned when necessary. Notification to the supervisory authority should form a part of that incident response plan.
7. The GDPR contains provisions on when a breach needs to be notified, and to whom, as well as what information should be provided as part of the notification. Information required for the notification can be provided in phases, but in any event controllers should act on any breach in a timely manner.
8. In its Opinion 03/2014 on personal data breach notification<sup>12</sup>, WP29 provided guidance to controllers in order to help them to decide whether to notify data subjects in case of a breach. The opinion considered the obligation of providers of electronic communications regarding Directive 2002/58/EC and provided examples from multiple sectors, in the context of the then draft GDPR, and presented good practices for all controllers.
9. The current Guidelines explain the mandatory breach notification and communication requirements of the GDPR and some of the steps controllers and processors can take to meet these obligations. They

---

<sup>6</sup> See [https://www.dataprotection.ie/docs/Data\\_Security\\_Breach\\_Code\\_of\\_Practice/1082.htm](https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm)

<sup>7</sup> See <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046>

<sup>8</sup> The rights enshrined in the Charter of Fundamental Rights of the EU, available at <http://eurlex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT>

<sup>9</sup> See Article 33(2) GDPR. This is similar in concept to Article 5 of Regulation (EU) No 611/2013 which states that a provider that is contracted to deliver part of an electronic communications service (without having a direct contractual relationship with subscribers) is obliged to notify the contracting provider in the event of a personal data breach.

<sup>10</sup> See Articles 34(4) and 58(2)(e) GDPR.

<sup>11</sup> This can be ensured under the monitoring and review requirement of a DPIA, which is required for processing operations likely to result in a high risk to the rights and freedoms of natural persons (Article 35(1) and (11)).

<sup>12</sup> See WP29 Opinion 03/2014 on Personal Data Breach Notification [http://ec.europa.eu/justice/data-protection/article29/documentation/opinion-recommendation/files/2014/wp213\\_en.pdf](http://ec.europa.eu/justice/data-protection/article29/documentation/opinion-recommendation/files/2014/wp213_en.pdf)

also give examples of various types of breaches and who would need to be notified in different scenarios.

## I. PERSONAL DATA BREACH NOTIFICATION UNDER THE GDPR

### A. Basic security considerations

10. One of the requirements of the GDPR is that, by using appropriate technical and organisational measures, personal data shall be processed in a manner to ensure the appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage<sup>13</sup>.
11. Accordingly, the GDPR requires both controllers and processors to have in place appropriate technical and organisational measures to ensure a level of security appropriate to the risk posed to the personal data being processed. They should take into account the state of the art, the costs of implementation and the nature, the scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons<sup>14</sup>. Also, the GDPR requires all appropriate technological protection and organisational measures to be in place to establish immediately whether a breach has taken place, which then determines whether the notification obligation is engaged<sup>15</sup>.
12. Consequently, a key element of any data security policy is being able, where possible, to prevent a breach and, where it nevertheless occurs, to react to it in a timely manner.

### B. What is a personal data breach?

#### 1. Definition

13. As part of any attempt to address a breach the controller should first be able to recognise one. The GDPR defines a “personal data breach” in Article 4(12) as:

*“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.”*

14. What is meant by “destruction” of personal data should be quite clear: this is where the data no longer exists, or no longer exists in a form that is of any use to the controller. “Damage” should also be relatively clear: this is where personal data has been altered, corrupted, or is no longer complete. In terms of “loss” of personal data, this should be interpreted as the data may still exist, but the controller has lost control or access to it, or no longer has it in its possession. Finally, unauthorised or unlawful processing may include disclosure of personal data to (or access by) recipients who are not authorised to receive (or access) the data, or any other form of processing which violates the GDPR.

#### Example

An example of loss of personal data can include where a device containing a copy of a controller’s customer database has been lost or stolen. A further example of loss may be where the only copy of a set of personal data has been encrypted by ransomware, or has been encrypted by the controller using a key that is no longer in its possession.

15. What should be clear is that a breach is a type of security incident. However, as indicated by Article 4(12), the GDPR only applies where there is a breach of personal data. The consequence of such a breach is that the controller will be unable to ensure compliance with the principles relating to the

---

<sup>13</sup> See Articles 5(1)(f) and 32 GDPR.

<sup>14</sup> Article 32; see also Recital 83 GDPR.

<sup>15</sup> See Recital 87 GDPR.

processing of personal data as outlined in Article 5 GDPR. This highlights the difference between a security incident and a personal data breach – in essence, whilst all personal data breaches are security incidents, not all security incidents are necessarily personal data breaches<sup>16</sup>.

16. The potential adverse effects of a breach on individuals are considered below.

## 2. Types of personal data breaches

17. In its Opinion 03/2014 on breach notification, WP29 explained that breaches can be categorised according to the following three well-known information security principles<sup>17</sup>:

- “**Confidentiality breach**” - where there is an unauthorised or accidental disclosure of, or access to, personal data.
- “**Integrity breach**” - where there is an unauthorised or accidental alteration of personal data.
- “**Availability breach**” - where there is an accidental or unauthorised loss of access<sup>18</sup> to, or destruction of, personal data.

18. It should also be noted that, depending on the circumstances, a breach can concern confidentiality, integrity and availability of personal data at the same time, as well as any combination of these.

19. Whereas determining if there has been a breach of confidentiality or integrity is relatively clear, whether there has been an availability breach may be less obvious. A breach will always be regarded as an availability breach when there has been a permanent loss of, or destruction of, personal data.

### Example

Examples of a loss of availability include where data has been deleted either accidentally or by an unauthorised person, or, in the example of securely encrypted data, the decryption key has been lost. In the event that the controller cannot restore access to the data, for example, from a backup, then this is regarded as a permanent loss of availability.

A loss of availability may also occur where there has been significant disruption to the normal service of an organisation, for example, experiencing a power failure or denial of service attack, rendering personal data unavailable.

20. The question may be asked whether a temporary loss of availability of personal data should be considered as a breach and, if so, one which needs to be notified. Article 32 GDPR, “security of processing”, explains that when implementing technical and organisational measures to ensure a level of security appropriate to the risk, consideration should be given, amongst other things, to “*the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and*

---

<sup>16</sup> It should be noted that a security incident is not limited to threat models where an attack is made on an organisation from an external source, but includes incidents from internal processing that breach security principles.

<sup>17</sup> See WP29 Opinion 03/2014.

<sup>18</sup> It is well established that “access” is fundamentally part of “availability”. See, for example, NIST SP800-53rev4, which defines “availability” as: “Ensuring timely and reliable access to and use of information,” available at <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>. CNSSI-4009 also refers to: “Timely, reliable access to data and information services for authorized users”. See <https://rmf.org/wpcontent/uploads/2017/10/CNSSI-4009.pdf>. ISO/IEC 27000:2016 also defines “availability” as “Property of being accessible and usable upon demand by an authorized entity”: <https://www.iso.org/obp/ui/#iso:std:isoiec:27000:ed-4:v1:en>

*services,” and “the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident”.*

21. Therefore, a security incident resulting in personal data being made unavailable for a period of time is also a type of breach, as the lack of access to the data can have a significant impact on the rights and freedoms of natural persons. To be clear, where personal data is unavailable due to planned system maintenance being carried out this is not a ‘breach of security’ as defined in Article 4(12) GDPR.
22. As with a permanent loss or destruction of personal data (or indeed any other type of breach), a breach involving the temporary loss of availability should be documented in accordance with Article 33(5) GDPR. This assists the controller in demonstrating accountability to the supervisory authority, which may ask to see those records<sup>19</sup>. However, depending on the circumstances of the breach, it may or may not require notification to the supervisory authority and communication to affected individuals. The controller will need to assess the likelihood and severity of the impact on the rights and freedoms of natural persons as a result of the lack of availability of personal data. In accordance with Article 33 GDPR, the controller will need to notify unless the breach is unlikely to result in a risk to individuals’ rights and freedoms. Of course, this will need to be assessed on a case-by-case basis.

**Example**

In the context of a hospital, if critical medical data about patients are unavailable, even temporarily, this could present a risk to individuals’ rights and freedoms; for example, operations may be cancelled and lives put at risk.

Conversely, in the case of a media company’s systems being unavailable for several hours (e.g. due to a power outage), if that company is then prevented from sending newsletters to its subscribers, this is unlikely to present a risk to individuals’ rights and freedoms.

23. It should be noted that although a loss of availability of a controller’s systems might be only temporary and may not have an impact on individuals, it is important for the controller to consider all possible consequences of a breach, as it may still require notification for other reasons.

**Example**

Infection by ransomware (malicious software which encrypts the controller’s data until a ransom is paid) could lead to a temporary loss of availability if the data can be restored from backup. However, a network intrusion still occurred, and notification could be required if the incident is qualified as confidentiality breach (i.e. personal data is accessed by the attacker) and this presents a risk to the rights and freedoms of individuals.

### **3. The possible consequences of a personal data breach**

24. A breach can potentially have a range of significant adverse effects on individuals, which can result in physical, material, or non-material damage. The GDPR explains that this can include loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, and loss of confidentiality of personal data protected by professional secrecy. It can also include any other significant economic or social disadvantage to those individuals<sup>20</sup>.
25. Accordingly, the GDPR requires the controller to notify a breach to the competent supervisory authority, unless it is unlikely to result in a risk of such adverse effects taking place. Where there is a

---

<sup>19</sup> See Article 33(5) GDPR.

<sup>20</sup> See also Recitals 85 and 75 GDPR.

likely high risk of these adverse effects occurring, the GDPR requires the controller to communicate the breach to the affected individuals as soon as is reasonably feasible<sup>21</sup>.

26. The importance of being able to identify a breach, to assess the risk to individuals, and then notify if required, is emphasised in Recital 87 of the GDPR:

*"It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation."*

27. Further guidelines on assessing the risk of adverse effects to individuals are considered in section IV.

28. If controllers fail to notify either the supervisory authority or data subjects of a data breach or both even though the requirements of Articles 33 and/or 34 GDPR are fulfilled, then the supervisory authority is presented with a choice that must include consideration of all of the corrective measures at its disposal, which would include consideration of the imposition of the appropriate administrative fine<sup>22</sup>, either accompanying a corrective measure under Article 58(2) GDPR or on its own. Where an administrative fine is chosen, its value can be up to 10,000,000 EUR or up to 2 % if the total worldwide annual turnover of an undertaking under Article 83(4)(a) of the GDPR. It is also important to bear in mind that in some cases, the failure to notify a breach could reveal either an absence of existing security measures or an inadequacy of the existing security measures. The WP29 Guidelines on administrative fines state: *"The occurrence of several different infringements committed together in any particular single case means that the supervisory authority is able to apply the administrative fines at a level which is effective, proportionate and dissuasive within the limit of the gravest infringement"*. In that case, the supervisory authority will also have the possibility to issue sanctions for failure to notify or communicate the breach (Articles 33 and 34 GDPR) on the one hand, and absence of (adequate) security measures (Article 32 GDPR) on the other hand, as they are two separate infringements.

## II. ARTICLE 33 - NOTIFICATION TO THE SUPERVISORY AUTHORITY

### A. When to notify

#### 1. Article 33 requirements

29. Article 33(1) GDPR provides that:

*"In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay."*

30. Recital 87 GDPR states<sup>23</sup>:

---

<sup>21</sup> See also Recital 86 GDPR.

<sup>22</sup> For further details, please see WP29 Guidelines on the application and setting of administrative fines, available here: [http://ec.europa.eu/newsroom/just/document.cfm?doc\\_id=47889](http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889)

<sup>23</sup> Recital 85 GDPR is also important here.

*"It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation."*

## 2. When does a controller become “aware”?

31. As detailed above, the GDPR requires that, in the case of a breach, the controller shall notify the breach without undue delay and, where feasible, not later than 72 hours after having become aware of it. This may raise the question of when a controller can be considered to have become “aware” of a breach. The EDPB considers that a controller should be regarded as having become “aware” when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised.
32. However, as indicated earlier, the GDPR requires the controller to implement all appropriate technical protection and organisational measures to establish immediately whether a breach has taken place and to inform promptly the supervisory authority and the data subjects. It also states that the fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the breach and its consequences and adverse effects for the data subject<sup>24</sup>. This puts an obligation on the controller to ensure that they will be “aware” of any breaches in a timely manner so that they can take appropriate action.
33. When, exactly, a controller can be considered to be “aware” of a particular breach will depend on the circumstances of the specific breach. In some cases, it will be relatively clear from the outset that there has been a breach, whereas in others, it may take some time to establish if personal data have been compromised. However, the emphasis should be on prompt action to investigate an incident to determine whether personal data have indeed been breached, and if so, to take remedial action and notify if required.

### Examples

1. In the case of a loss of a USB key with unencrypted personal data it is often not possible to ascertain whether unauthorised persons gained access to that data. Nevertheless, even though the controller may not be able to establish if a confidentiality breach has taken place, such a case has to be notified as there is a reasonable degree of certainty that an availability breach has occurred; the controller would become “aware” when it realised the USB key had been lost.
2. A third party informs a controller that they have accidentally received the personal data of one of its customers and provides evidence of the unauthorised disclosure. As the controller has been presented with clear evidence of a confidentiality breach then there can be no doubt that it has become “aware”.
3. A controller detects that there has been a possible intrusion into its network. The controller checks its systems to establish whether personal data held on that system has been compromised and confirms this is the case. Once again, as the controller now has clear evidence of a breach there can be no doubt that it has become “aware”.

---

<sup>24</sup> See Recital 87 GDPR.

4. A cybercriminal contacts the controller after having hacked its system in order to ask for a ransom. In that case, after checking its system to confirm it has been attacked the controller has clear evidence that a breach has occurred and there is no doubt that it has become aware.

34. After first being informed of a potential breach by an individual, a media organisation, or another source, or when it has itself detected a security incident, the controller may undertake a short period of investigation in order to establish whether or not a breach has in fact occurred. During this period of investigation the controller may not be regarded as being “aware”. However, it is expected that the initial investigation should begin as soon as possible and establish with a reasonable degree of certainty whether a breach has taken place; a more detailed investigation can then follow.
35. Once the controller has become aware, a notifiable breach must be notified without undue delay, and where feasible, not later than 72 hours. During this period, the controller should assess the likely risk to individuals in order to determine whether the requirement for notification has been triggered, as well as the action(s) needed to address the breach. However, a controller may already have an initial assessment of the potential risk that could result from a breach as part of a data protection impact assessment (DPIA)<sup>25</sup> made prior to carrying out the processing operation concerned. However, the DPIA may be more generalised in comparison to the specific circumstances of any actual breach, and so in any event an additional assessment taking into account those circumstances will need to be made. For more detail on assessing risk, see section IV.
36. In most cases these preliminary actions should be completed soon after the initial alert (i.e. when the controller or processor suspects there has been a security incident which may involve personal data.) – it should take longer than this only in exceptional cases.

**Example**

An individual informs the controller that they have received an email impersonating the controller which contains personal data relating to his (actual) use of the controller’s service, suggesting that the security of the controller has been compromised. The controller conducts a short period of investigation and identifies an intrusion into their network and evidence of unauthorised access to personal data. The controller would now be considered as “aware” and notification to the supervisory authority is required unless this is unlikely to present a risk to the rights and freedoms of individuals. The controller will need to take appropriate remedial action to address the breach.

37. The controller should therefore have internal processes in place to be able to detect and address a breach. For example, for finding some irregularities in data processing the controller or processor may use certain technical measures such as data flow and log analysers, from which is possible to define events and alerts by correlating any log data<sup>26</sup>. It is important that when a breach is detected it is reported upwards to the appropriate level of management so it can be addressed and, if required, notified in accordance with Article 33 and, if necessary, Article 34. Such measures and reporting mechanisms could be detailed in the controller’s incident response plans and/or governance arrangements. These will help the controller to plan effectively and determine who has operational responsibility within the organisation for managing a breach and how or whether to escalate an incident as appropriate.
38. The controller should also have in place arrangements with any processors the controller uses, which themselves have an obligation to notify the controller in the event of a breach (see below).

---

<sup>25</sup> See WP29 Guidelines WP248 on DPIAs here: [http://ec.europa.eu/newsroom/document.cfm?doc\\_id=44137](http://ec.europa.eu/newsroom/document.cfm?doc_id=44137)

<sup>26</sup> It should be noted that log data facilitating auditability of, e.g., storage, modifications or erasure of data may also qualify as personal data relating to the person who initiated the respective processing operation.

39. Whilst it is the responsibility of controllers and processors to put in place suitable measures to be able to prevent, react and address a breach, there are some practical steps that should be taken in all cases.

- Information concerning all security-related events should be directed towards a responsible person or persons with the task of addressing incidents, establishing the existence of a breach and assessing risk.
- Risk to individuals as a result of a breach should then be assessed (likelihood of no risk, risk or high risk), with relevant sections of the organisation being informed.
- Notification to the supervisory authority, and potentially communication of the breach to the affected individuals should be made, if required.
- At the same time, the controller should act to contain and recover the breach. Documentation of the breach should take place as it develops.

40. Accordingly, it should be clear that there is an obligation on the controller to act on any initial alert and establish whether or not a breach has, in fact, occurred. This brief period allows for some investigation, and for the controller to gather evidence and other relevant details. However, once the controller has established with a reasonable degree of certainty that a breach has occurred, if the conditions in Article 33(1) GDPR have been met, it must then notify the supervisory authority without undue delay and, where feasible, not later than 72 hours<sup>27</sup>. If a controller fails to act in a timely manner and it becomes apparent that a breach did occur, this could be considered as a failure to notify in accordance with Article 33 GDPR.

41. Article 32 GDPR makes clear that the controller and processor should have appropriate technical and organisational measures in place to ensure an appropriate level of security of personal data: the ability to detect, address, and report a breach in a timely manner should be seen as essential elements of these measures.

### 3. Joint controllers

42. Article 26 GDPR concerns joint controllers and specifies that joint controllers shall determine their respective responsibilities for compliance with the GDPR<sup>28</sup>. This will include determining which party will have responsibility for complying with the obligations under Articles 33 and 34 GDPR. The EDPB recommends that the contractual arrangements between joint controllers include provisions that determine which controller will take the lead on, or be responsible for, compliance with the GDPR's breach notification obligations.

### 4. Processor obligations

43. The controller retains overall responsibility for the protection of personal data, but the processor has an important role to play to enable the controller to comply with its obligations; and this includes breach notification. Indeed, Article 28(3) GDPR specifies that the processing by a processor shall be governed by a contract or other legal act. Article 28(3)(f) states that the contract or other legal act shall stipulate that the processor "assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor".

44. Article 33(2) GDPR makes it clear that if a processor is used by a controller and the processor becomes aware of a breach of the personal data it is processing on behalf of the controller, it must notify the controller "without undue delay". It should be noted that the processor does not need to first assess the likelihood of risk arising from a breach before notifying the controller; it is the controller that must make this assessment on becoming aware of the breach. The processor just needs to establish whether

---

<sup>27</sup> See Regulation No 1182/71 determining the rules applicable to periods, dates and time limits, available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31971R1182&from=EN>

<sup>28</sup> See also Recital 79 GDPR.

a breach has occurred and then notify the controller. The controller uses the processor to achieve its purposes; therefore, in principle, the controller should be considered as “aware” once the processor has informed it of the breach. The obligation on the processor to notify its controller allows the controller to address the breach and to determine whether or not it is required to notify the supervisory authority in accordance with Article 33(1) and the affected individuals in accordance with Article 34(1). The controller might also want to investigate the breach, as the processor might not be in a position to know all the relevant facts relating to the matter, for example, if a copy or backup of personal data destroyed or lost by the processor is still held by the controller. This may affect whether the controller would then need to notify.

45. The GDPR does not provide an explicit time limit within which the processor must alert the controller, except that it must do so “without undue delay”. Therefore, the EDPB recommends the processor promptly notifies the controller, with further information about the breach provided in phases as more details become available. This is important in order to help the controller to meet the requirement of notification to the supervisory authority within 72 hours.
46. As is explained above, the contract between the controller and processor should specify how the requirements expressed in Article 33(2) should be met in addition to other provisions in the GDPR. This can include requirements for early notification by the processor that in turn support the controller’s obligations to report to the supervisory authority within 72 hours.
47. Where the processor provides services to multiple controllers that are all affected by the same incident, the processor will have to report details of the incident to each controller.
48. A processor could make a notification on behalf of the controller, if the controller has given the processor the proper authorisation and this is part of the contractual arrangements between controller and processor. Such notification must be made in accordance with Article 33 and 34 GDPR. However, it is important to note that the legal responsibility to notify remains with the controller.

## B. Providing information to the supervisory authority

### 1. Information to be provided

49. When a controller notifies a breach to the supervisory authority, Article 33(3) GDPR states that, at the minimum, it should:

*“(a) describe 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;*

*(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;*

*(c) describe the likely consequences of the personal data breach;*

*(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.”*

50. The GDPR does not define categories of data subjects or personal data records. However, the EDPB suggests categories of data subjects to refer to the various types of individuals whose personal data has been affected by a breach: depending on the descriptors used, this could include, amongst others, children and other vulnerable groups, people with disabilities, employees or customers. Similarly, categories of personal data records can refer to the different types of records that the controller may process, such as health data, educational records, social care information, financial details, bank account numbers, passport numbers and so on.

51. Recital 85 GDPR makes it clear that one of the purposes of notification is limiting damage to individuals. Accordingly, if the types of data subjects or the types of personal data indicate a risk of particular damage occurring as a result of a breach (e.g. identity theft, fraud, financial loss, threat to professional secrecy), then it is important the notification indicates these categories. In this way, it is linked to the requirement of describing the likely consequences of the breach.
52. Where precise information is not available (e.g. exact number of data subjects affected) this should not be a barrier to timely breach notification. The GDPR allows for approximations to be made in the number of individuals affected and the number of personal data records concerned. The focus should be directed towards addressing the adverse effects of the breach rather than providing precise figures.
53. Thus, when it has become clear that there has been a breach, but the extent of it is not yet known, a notification in phases (see below) is a safe way to meet the notification obligations.
54. Article 33(3) GDPR states that the controller “shall at least” provide this information with a notification, so a controller can, if necessary, choose to provide further details. Different types of breaches (confidentiality, integrity or availability) might require further information to be provided to fully explain the circumstances of each case.

**Example**

As part of its notification to the supervisory authority, a controller may find it useful to name its processor if it is at the root cause of a breach, particularly if this has led to an incident affecting the personal data records of many other controllers that use the same processor.

55. In any event, the supervisory authority may request further details as part of its investigation into a breach.

## 2. Notification in phases

56. Depending on the nature of a breach, further investigation by the controller may be necessary to establish all of the relevant facts relating to the incident. Article 33(4) GDPR therefore states:

*“Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.”*

57. This means that the GDPR recognises that controllers will not always have all of the necessary information concerning a breach within 72 hours of becoming aware of it, as full and comprehensive details of the incident may not always be available during this initial period. As such, it allows for a notification in phases. It is more likely this will be the case for more complex breaches, such as some types of cyber security incidents where, for example, an in-depth forensic investigation may be necessary to fully establish the nature of the breach and the extent to which personal data have been compromised. Consequently, in many cases the controller will have to do more investigation and follow-up with additional information at a later point. This is permissible, providing the controller gives reasons for the delay, in accordance with Article 33(1) GDPR. The EDPB recommends that when the controller first notifies the supervisory authority, the controller should also inform the supervisory authority if the controller does not yet have all the required information and will provide more details later on. The supervisory authority should agree how and when additional information should be provided. This does not prevent the controller from providing further information at any other stage, if it becomes aware of additional relevant details about the breach that need to be provided to the supervisory authority.

58. The focus of the notification requirement is to encourage controllers to act promptly on a breach, contain it and, if possible, recover the compromised personal data, and to seek relevant advice from the supervisory authority. Notifying the supervisory authority within the first 72 hours can allow the controller to make sure that decisions about notifying or not notifying individuals are correct.

59. However, the purpose of notifying the supervisory authority is not solely to obtain guidance on whether to notify the affected individuals. It will be obvious in some cases that, due to the nature of the breach and the severity of the risk, the controller will need to notify the affected individuals without delay. For example, if there is an immediate threat of identity theft, or if special categories of personal data<sup>29</sup> are disclosed online, the controller should act without undue delay to contain the breach and to communicate it to the individuals concerned (see section III). In exceptional circumstances, this might even take place before notifying the supervisory authority. More generally, notification of the supervisory authority may not serve as a justification for failure to communicate the breach to the data subject where it is required.
60. It should also be clear that after making an initial notification, a controller could update the supervisory authority if a follow-up investigation uncovers evidence that the security incident was contained and no breach actually occurred. This information could then be added to the information already given to the supervisory authority and the incident recorded accordingly as not being a breach. There is no penalty for reporting an incident that ultimately transpires not to be a breach.

**Example**

A controller notifies the supervisory authority within 72 hours of detecting a breach that it has lost a USB key containing a copy of the personal data of some of its customers. The USB key is later found misfiled within the controller's premises and recovered. The controller updates the supervisory authority and requests the notification be amended.

61. It should be noted that a phased approach to notification is already the case under the existing obligations of Directive 2002/58/EC, Regulation 611/2013 and other self-reported incidents.

### [3. Delayed notifications](#)

62. Article 33(1) GDPR makes it clear that where notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. This, along with the concept of notification in phases, recognises that a controller may not always be able to notify a breach within that time period, and that a delayed notification may be permissible.
63. Such a scenario might take place where, for example, a controller experiences multiple, similar confidentiality breaches over a short period of time, affecting large numbers of data subjects in the same way. A controller could become aware of a breach and, whilst beginning its investigation, and before notification, detect further similar breaches, which have different causes. Depending on the circumstances, it may take the controller some time to establish the extent of the breaches and, rather than notify each breach individually, the controller instead organises a meaningful notification that represents several very similar breaches, with possible different causes. This could lead to notification to the supervisory authority being delayed by more than 72 hours after the controller first becomes aware of these breaches.
64. Strictly speaking, each individual breach is a reportable incident. However, to avoid being overly burdensome, the controller may be able to submit a "bundled" notification representing all these breaches, provided that they concern the same type of personal data breached in the same way, over a relatively short space of time. If a series of breaches take place that concern different types of personal data, breached in different ways, then notification should proceed in the normal way, with each breach being reported in accordance with Article 33.

---

<sup>29</sup> See Article 9 GDPR.

65. Whilst the GDPR allows for delayed notifications to an extent, this should not be seen as something that regularly takes place. It is worth pointing out that bundled notifications can also be made for multiple similar breaches reported within 72 hours.

### C. Cross-border breaches and breaches at non-EU establishments

#### 1. Cross-border breaches

66. Where there is cross-border processing<sup>30</sup> of personal data, a breach may affect data subjects in more than one Member State. Article 33(1) GDPR makes it clear that when a breach has occurred, the controller should notify the supervisory authority competent in accordance with Article 55 of the GDPR<sup>31</sup>. Article 55(1) GDPR says that:

*"Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State."*

67. However, Article 56(1) GDPR states:

*"Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60."*

68. Furthermore, Article 56(6) GDPR states:

*"The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor."*

69. This means that whenever a breach takes place in the context of cross-border processing and notification is required, the controller will need to notify the lead supervisory authority<sup>32</sup>. Therefore, when drafting its breach response plan, a controller must make an assessment as to which supervisory authority is the lead supervisory authority that it will need to notify<sup>33</sup>. This will allow the controller to respond promptly to a breach and to meet its obligations in respect of Article 33. It should be clear that in the event of a breach involving cross-border processing, notification must be made to the lead supervisory authority, which is not necessarily where the affected data subjects are located, or indeed where the breach has taken place. When notifying the lead authority, the controller should indicate, where appropriate, whether the breach involves establishments located in other Member States, and in which Member States data subjects are likely to have been affected by the breach. If the controller has any doubt as to the identity of the lead supervisory authority then it should, at a minimum, notify the local supervisory authority where the breach has taken place.

#### 2. Breaches at non-EU establishments

70. Article 3 GDPR concerns the territorial scope of the GDPR, including when it applies to the processing of personal data by a controller or processor that is not established in the EU. In particular, Article 3(2) GDPR states<sup>34</sup>:

---

<sup>30</sup> See Article 4(23) GDPR.

<sup>31</sup> See also Recital 122 GDPR.

<sup>32</sup> See WP29 Guidelines for identifying a controller or processor's lead supervisory authority, available at [http://ec.europa.eu/newsroom/document.cfm?doc\\_id=44102](http://ec.europa.eu/newsroom/document.cfm?doc_id=44102)

<sup>33</sup> A list of contact details for all European national data protection authorities can be found at: [https://edpb.europa.eu/about-edpb/about-edpb/members\\_en](https://edpb.europa.eu/about-edpb/about-edpb/members_en)

<sup>34</sup> See also Recitals 23 and 24 GDPR.

*"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."*

71. Article 3(3) GDPR is also relevant and states<sup>35</sup>:

*"This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law."*

- 72. Where a controller not established in the EU is subject to Article 3(2) or Article 3(3) GDPR and experiences a breach, it is therefore still bound by the notification obligations under Articles 33 and 34 GDPR. Article 27 GDPR requires a controller (and a processor) to designate a representative in the EU where Article 3(2) GDPR applies.
- 73. However, the mere presence of a representative in a Member State does not trigger the one-stop-shop system.<sup>36</sup> For this reason the breach will need to be notified to every supervisory authority for which affected data subjects reside in their Member State. This (These) notification(s) shall be the responsibility of the controller.<sup>37</sup>
- 74. Similarly, where a processor is subject to Article 3(2) GDPR, it will be bound by the obligations on processors, of particular relevance here, the duty to notify a breach to the controller under Article 33(2) GDPR.

#### D. Conditions where notification is not required

- 75. Article 33(1) GDPR makes it clear that breaches that are "unlikely to result in a risk to the rights and freedoms of natural persons" do not require notification to the supervisory authority. An example might be where personal data are already publicly available and a disclosure of such data does not constitute a likely risk to the individual. This is in contrast to existing breach notification requirements for providers of publicly available electronic communications services in Directive 2009/136/EC that state all relevant breaches have to be notified to the competent authority.
- 76. In its Opinion 03/2014 on breach notification<sup>38</sup>, WP29 explained that a confidentiality breach of personal data that were encrypted with a state of the art algorithm is still a personal data breach, and has to be notified. However, if the confidentiality of the key is intact – i.e., the key was not compromised in any security breach, and was generated so that it cannot be ascertained by available technical means by any person who is not authorised to access it – then the data are in principle unintelligible. Thus, the breach is unlikely to adversely affect individuals and therefore would not

---

<sup>35</sup> See also Recital 25 GDPR.

<sup>36</sup> See WP29 Guidelines for identifying a controller or processor's lead supervisory authority, available at [http://ec.europa.eu/newsroom/document.cfm?doc\\_id=44102](http://ec.europa.eu/newsroom/document.cfm?doc_id=44102)

<sup>37</sup> In line with guidelines 3/2018 on the territorial scope of the GDPR (Article 3), available at [https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version\\_en](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en), the EDPA considers the function of a representative in the Union as not compatible with the role of an external data protection officer ("DPO"), therefore the responsibility to notify the supervisory authority in case of a personal data breach remains that of the controller in line with Article 27(5) GDPR. A representative can however be involved in the notification process if this has been explicitly stipulated in the written mandate.

<sup>38</sup> WP29, Opinion 03/2014 on breach notification, [http://ec.europa.eu/justice/data-protection/article29/documentation/opinion-recommendation/files/2014/wp213\\_en.pdf](http://ec.europa.eu/justice/data-protection/article29/documentation/opinion-recommendation/files/2014/wp213_en.pdf)

require communication to those individuals<sup>39</sup>. However, even where data is encrypted, a loss or alteration can have negative consequences for data subjects where the controller has no adequate backups. In that instance communication to data subjects would be required, even if the data itself was subject to adequate encryption measures.

77. WP29 also explained this would similarly be the case if personal data, such as passwords, were securely hashed and salted, the hashed value was calculated with a state of the art cryptographic keyed hash function, the key used to hash the data was not compromised in any breach, and the key used to hash the data has been generated in a way that it cannot be ascertained by available technological means by any person who is not authorised to access it.
78. Consequently, if personal data have been made essentially unintelligible to unauthorised parties and where the data are a copy or a backup exists, a confidentiality breach involving properly encrypted personal data may not need to be notified to the supervisory authority. This is because such a breach is unlikely to pose a risk to individuals' rights and freedoms. This of course means that the individual would not need to be informed either as there is likely no high risk. However, it should be borne in mind that while notification may initially not be required if there is no likely risk to the rights and freedoms of individuals, this may change over time and the risk would have to be re-evaluated. For example, if the key is subsequently found to be compromised, or a vulnerability in the encryption software is exposed, then notification may still be required.
79. Furthermore, it should be noted that if there is a breach where there are no backups of the encrypted personal data then there will have been an availability breach, which could pose risks to individuals and therefore may require notification. Similarly, where a breach occurs involving the loss of encrypted data, even if a backup of the personal data exists this may still be a reportable breach, depending on the length of time taken to restore the data from that backup and the effect that lack of availability has on individuals. As Article 32(1)(c) GDPR states, an important factor of security is the "*the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident*".

#### **Example**

A breach that would not require notification to the supervisory authority would be the loss of a securely encrypted mobile device, utilised by the controller and its staff. Provided the encryption key remains within the secure possession of the controller and this is not the sole copy of the personal data then the personal data would be inaccessible to an attacker. This means the breach is unlikely to result in a risk to the rights and freedoms of the data subjects in question. If it later becomes evident that the encryption key was compromised or that the encryption software or algorithm is vulnerable, then the risk to the rights and freedoms of natural persons will change and thus notification may now be required.

80. However, a failure to comply with Article 33 GDPR will exist where a controller does not notify the supervisory authority in a situation where the data has not actually been securely encrypted. Therefore, when selecting encryption software controllers should carefully weigh the quality and the proper implementation of the encryption offered, understand what level of protection it actually provides and whether this is appropriate to the risks presented. Controllers should also be familiar with the specifics of how their encryption product functions. For instance, a device may be encrypted once it is switched off, but not while it is in stand-by mode. Some products using encryption have "default keys" that need to be changed by each customer to be effective. The encryption may also be considered currently adequate by security experts, but may become outdated in a few years' time,

---

<sup>39</sup> See also Article 4(1) and (2) of Regulation 611/2013.

meaning it is questionable whether the data would be sufficiently encrypted by that product and provide an appropriate level of protection.

### III. ARTICLE 34 – COMMUNICATION TO THE DATA SUBJECT

#### A. Informing individuals

81. In certain cases, as well as notifying the supervisory authority, the controller is also required to communicate a breach to the affected individuals.

Article 34(1) GDPR states:

*"When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay."*

82. Controllers should recall that notification to the supervisory authority is mandatory unless there is unlikely to be a risk to the rights and freedoms of individuals as a result of a breach. In addition, where there is likely a high risk to the rights and freedoms of individuals as the result of a breach, individuals must also be informed. The threshold for communicating a breach to individuals is therefore higher than for notifying supervisory authorities and not all breaches will therefore be required to be communicated to individuals, thus protecting them from unnecessary notification fatigue.
83. The GDPR states that communication of a breach to individuals should be made "without undue delay," which means as soon as possible. The main objective of notification to individuals is to provide specific information about steps they should take to protect themselves<sup>40</sup>. As noted above, depending on the nature of the breach and the risk posed, timely communication will help individuals to take steps to protect themselves from any negative consequences of the breach.
84. Annex B of these Guidelines provides a non-exhaustive list of examples of when a breach may be likely to result in high risk to individuals and consequently instances when a controller will have to notify a breach to those affected.

#### B. Information to be provided

85. When notifying individuals, Article 34(2) GDPR specifies that:

*"The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3)."*

86. According to this provision, the controller should at least provide the following information:

- a description of the nature of the breach;
- the name and contact details of the data protection officer or other contact point;
- a description of the likely consequences of the breach; and
- a description of the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

87. As an example of the measures taken to address the breach and to mitigate its possible adverse effects, the controller could state that, after having notified the breach to the relevant supervisory authority, the controller has received advice on managing the breach and lessening its impact. The controller should also, where appropriate, provide specific advice to individuals to protect themselves from

---

<sup>40</sup> See also Recital 86 GDPR.

possible adverse consequences of the breach, such as resetting passwords in the case where their access credentials have been compromised. Again, a controller can choose to provide information in addition to what is required here.

### C. Contacting individuals

88. In principle, the relevant breach should be communicated to the affected data subjects directly, unless doing so would involve a disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner (Article 34(3)(c) GDPR).
89. Dedicated messages should be used when communicating a breach to data subjects and they should not be sent with other information, such as regular updates, newsletters, or standard messages. This helps to make the communication of the breach to be clear and transparent.
90. Examples of transparent communication methods include direct messaging (e.g. email, SMS, direct message), prominent website banners or notification, postal communications and prominent advertisements in print media. A notification solely confined within a press release or corporate blog would not be an effective means of communicating a breach to an individual. The EDPB recommends that controllers should choose a means that maximizes the chance of properly communicating information to all affected individuals. Depending on the circumstances, this may mean the controller employs several methods of communication, as opposed to using a single contact channel.
91. Controllers may also need to ensure that the communication is accessible in appropriate alternative formats and relevant languages to ensure individuals are able to understand the information being provided to them. For example, when communicating a breach to an individual, the language used during the previous normal course of business with the recipient will generally be appropriate. However, if the breach affects data subjects who the controller has not previously interacted with, or particularly those who reside in a different Member State or other non-EU country from where the controller is established, communication in the local national language could be acceptable, taking into account the resource required. The key is to help data subjects understand the nature of the breach and steps they can take to protect themselves.
92. Controllers are best placed to determine the most appropriate contact channel to communicate a breach to individuals, particularly if they interact with their customers on a frequent basis. However, clearly a controller should be wary of using a contact channel compromised by the breach as this channel could also be used by attackers impersonating the controller.
93. At the same time, Recital 86 GDPR explains that:

*"Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication."*

94. Controllers might therefore wish to contact and consult the supervisory authority not only to seek advice about informing data subjects about a breach in accordance with Article 34, but also on the appropriate messages to be sent to, and the most appropriate way to contact, individuals.
95. Linked to this is the advice given in Recital 88 GDPR that notification of a breach should "take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach". This may mean that in certain circumstances, where justified, and on the advice of law-enforcement authorities, the controller may delay communicating the breach to the affected individuals until such time as it

would not prejudice such investigations. However, data subjects would still need to be promptly informed after this time.

96. Whenever it is not possible for the controller to communicate a breach to an individual because there is insufficient data stored to contact the individual, in that particular circumstance the controller should inform the individual as soon as it is reasonably feasible to do so (e.g. when an individual exercises their Article 15 right to access personal data and provides the controller with necessary additional information to contact them).

#### D. Conditions where communication is not required

97. Article 34(3) GDPR states three conditions that, if met, do not require notification to individuals in the event of a breach. These are:

- The controller has applied appropriate technical and organisational measures to protect personal data prior to the breach, in particular those measures that render personal data unintelligible to any person who is not authorised to access it. This could, for example, include protecting personal data with state-of-the-art encryption, or by tokenization.
- Immediately following a breach, the controller has taken steps to ensure that the high risk posed to individuals' rights and freedoms is no longer likely to materialise. For example, depending on the circumstances of the case, the controller may have immediately identified and taken action against the individual who has accessed personal data before they were able to do anything with it. Due regard still needs to be given to the possible consequences of any breach of confidentiality, again, depending on the nature of the data concerned.
- It would involve disproportionate effort<sup>41</sup> to contact individuals, perhaps where their contact details have been lost as a result of the breach or are not known in the first place. For example, the warehouse of a statistical office has flooded and the documents containing personal data were stored only in paper form. Instead, the controller must make a public communication or take a similar measure, whereby the individuals are informed in an equally effective manner. In the case of disproportionate effort, technical arrangements could also be envisaged to make information about the breach available on demand, which could prove useful to those individuals who may be affected by a breach, but the controller cannot otherwise contact.

98. In accordance with the accountability principle controllers should be able to demonstrate to the supervisory authority that they meet one or more of these conditions<sup>42</sup>. It should be borne in mind that while notification may initially not be required if there is no risk to the rights and freedoms of natural persons, this may change over time and the risk would have to be re-evaluated.

99. If a controller decides not to communicate a breach to the individual, Article 34(4) GDPR explains that the supervisory authority can require it to do so, if it considers the breach is likely to result in a high risk to individuals. Alternatively, it may consider that the conditions in Article 34(3) GDPR have been met in which case notification to individuals is not required. If the supervisory authority determines that the decision not to notify data subjects is not well founded, it may consider employing its available powers and sanctions.

---

<sup>41</sup> See WP29 Guidelines on transparency, which will consider the issue of disproportionate effort, available at [http://ec.europa.eu/newsroom/just/document.cfm?doc\\_id=48850](http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850)

<sup>42</sup> See Article 5(2) GDPR.

## IV. ASSESSING RISK AND HIGH RISK

### A. Risk as a trigger for notification

100. Although the GDPR introduces the obligation to notify a breach, it is not a requirement to do so in all circumstances:

- Notification to the competent supervisory authority is required unless a breach is unlikely to result in a risk to the rights and freedoms of individuals.
- Communication of a breach to the individual is only triggered where it is likely to result in a high risk to their rights and freedoms.

101. This means that immediately upon becoming aware of a breach, it is vitally important that the controller should not only seek to contain the incident but it should also assess the risk that could result from it. There are two important reasons for this: firstly, knowing the likelihood and the potential severity of the impact on the individual will help the controller to take effective steps to contain and address the breach; secondly, it will help it to determine whether notification is required to the supervisory authority and, if necessary, to the individuals concerned.

102. As explained above, notification of a breach is required unless it is unlikely to result in a risk to the rights and freedoms of individuals, and the key trigger requiring communication of a breach to data subjects is where it is likely to result in a *high* risk to the rights and freedoms of individuals. This risk exists when the breach may lead to physical, material or non-material damage for the individuals whose data have been breached. Examples of such damage are discrimination, identity theft or fraud, financial loss and damage to reputation. When the breach involves personal data that reveals racial or ethnic origin, political opinion, religion or philosophical beliefs, or trade union membership, or includes genetic data, data concerning health or data concerning sex life, or criminal convictions and offences or related security measures, such damage should be considered likely to occur<sup>43</sup>.

### B. Factors to consider when assessing risk

103. Recitals 75 and 76 of the GDPR suggest that generally when assessing risk, consideration should be given to both the likelihood and severity of the risk to the rights and freedoms of data subjects. It further states that risk should be evaluated on the basis of an objective assessment.

104. It should be noted that assessing the risk to people's rights and freedoms as a result of a breach has a different focus to the risk considered in a DPIA)<sup>44</sup>. The DPIA considers both the risks of the data processing being carried out as planned, and the risks in case of a breach. When considering a potential breach, it looks in general terms at the likelihood of this occurring, and the damage to the data subject that might ensue; in other words, it is an assessment of a hypothetical event. With an actual breach, the event has already occurred, and so the focus is wholly about the resulting risk of the impact of the breach on individuals.

#### Example

A DPIA suggests that the proposed use of a particular security software product to protect personal data is a suitable measure to ensure a level of security appropriate to the risk the processing would otherwise present to individuals. However, if a vulnerability becomes subsequently known, this would change the software's suitability to contain the risk to the personal data protected and so it would need to be re-assessed as part of an ongoing DPIA. A vulnerability in the product is later exploited and

<sup>43</sup> See Recital 75 and Recital 85 GDPR.

<sup>44</sup> See WP Guidelines on DPIAs here: [http://ec.europa.eu/newsroom/document.cfm?doc\\_id=44137](http://ec.europa.eu/newsroom/document.cfm?doc_id=44137)

a breach occurs. The controller should assess the specific circumstances of the breach, the data affected, and the potential level of impact on individuals, as well as how likely this risk will materialise.

105. Accordingly, when assessing the risk to individuals as a result of a breach, the controller should consider the specific circumstances of the breach, including the severity of the potential impact and the likelihood of this occurring. The EDPB therefore recommends the assessment should take into account the following criteria<sup>45</sup>:

- **The type of breach**

106. The type of breach that has occurred may affect the level of risk presented to individuals. For example, a confidentiality breach whereby medical information has been disclosed to unauthorised parties may have a different set of consequences for an individual to a breach where an individual's medical details have been lost, and are no longer available.

- **The nature, sensitivity, and volume of personal data**

107. Of course, when assessing risk, a key factor is the type and sensitivity of personal data that has been compromised by the breach. Usually, the more sensitive the data, the higher the risk of harm will be to the people affected, but consideration should also be given to other personal data that may already be available about the data subject. For example, the disclosure of the name and address of an individual in ordinary circumstances is unlikely to cause substantial damage. However, if the name and address of an adoptive parent is disclosed to a birth parent, the consequences could be very severe for both the adoptive parent and child.

108. Breaches involving health data, identity documents, or financial data such as credit card details, can all cause harm on their own, but if used together they could be used for identity theft. A combination of personal data is typically more sensitive than a single piece of personal data.

109. Some types of personal data may seem at first relatively innocuous, however, what that data may reveal about the affected individual should be carefully considered. A list of customers accepting regular deliveries may not be particularly sensitive, but the same data about customers who have requested that their deliveries be stopped while on holiday would be useful information to criminals.

110. Similarly, a small amount of highly sensitive personal data can have a high impact on an individual, and a large range of details can reveal a greater range of information about that individual. Also, a breach affecting large volumes of personal data about many data subjects can have an effect on a corresponding large number of individuals.

- **Ease of identification of individuals**

111. An important factor to consider is how easy it will be for a party who has access to compromised personal data to identify specific individuals, or match the data with other information to identify individuals. Depending on the circumstances, identification could be possible directly from the personal data breached with no special research needed to discover the individual's identity, or it may be extremely difficult to match personal data to a particular individual, but it could still be possible under certain conditions. Identification may be directly or indirectly possible from the breached data, but it may also depend on the specific context of the breach, and public availability of related personal details. This may be more relevant for confidentiality and availability breaches.

---

<sup>45</sup> Article 3.2 of Regulation 611/2013 provides guidance the factors that should be taken into consideration in relation to the notification of breaches in the electronic communication services sector, which may be useful in the context of notification under the GDPR. See <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF>

112. As stated above, personal data protected by an appropriate level of encryption will be unintelligible to unauthorised persons without the decryption key. Additionally, appropriately-implemented pseudonymisation (defined in Article 4(5) GDPR as "*the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*") can also reduce the likelihood of individuals being identified in the event of a breach. However, pseudonymisation techniques alone cannot be regarded as making the data unintelligible.

- **Severity of consequences for individuals**

113. Depending on the nature of the personal data involved in a breach, for example, special categories of data, the potential damage to individuals that could result can be especially severe, in particular where the breach could result in identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation. If the breach concerns personal data about vulnerable individuals, they could be placed at greater risk of harm.

114. Whether the controller is aware that personal data is in the hands of people whose intentions are unknown or possibly malicious can have a bearing on the level of potential risk. There may be a confidentiality breach, whereby personal data is disclosed to a third party, as defined in Article 4(10), or other recipient in error. This may occur, for example, where personal data is sent accidentally to the wrong department of an organisation, or to a commonly used supplier organisation. The controller may request the recipient to either return or securely destroy the data it has received. In both cases, given that the controller has an ongoing relationship with them, and it may be aware of their procedures, history and other relevant details, the recipient may be considered "trusted". In other words, the controller may have a level of assurance with the recipient so that it can reasonably expect that party not to read or access the data sent in error, and to comply with its instructions to return it. Even if the data has been accessed, the controller could still possibly trust the recipient not to take any further action with it and to return the data to the controller promptly and to co-operate with its recovery. In such cases, this may be factored into the risk assessment the controller carries out following the breach – the fact that the recipient is trusted may eradicate the severity of the consequences of the breach but does not mean that a breach has not occurred. However, this in turn may remove the likelihood of risk to individuals, thus no longer requiring notification to the supervisory authority, or to the affected individuals. Again, this will depend on case-by-case basis. Nevertheless, the controller still has to keep information concerning the breach as part of the general duty to maintain records of breaches (see section V, below).

115. Consideration should also be given to the permanence of the consequences for individuals, where the impact may be viewed as greater if the effects are long-term.

- **Special characteristics of the individual**

116. A breach may affect personal data concerning children or other vulnerable individuals, who may be placed at greater risk of danger as a result. There may be other factors about the individual that may affect the level of impact of the breach on them.

- **Special characteristics of the data controller**

117. The nature and role of the controller and its activities may affect the level of risk to individuals as a result of a breach. For example, a medical organisation will process special categories of personal data, meaning that there is a greater threat to individuals if their personal data is breached, compared with a mailing list of a newspaper.

- **The number of affected individuals**

118. A breach may affect only one or a few individuals or several thousand, if not many more. Generally, the higher the number of individuals affected, the greater the impact of a breach can have. However, a breach can have a severe impact on even one individual, depending on the nature of the personal data and the context in which it has been compromised. Again, the key is to consider the likelihood and severity of the impact on those affected.

- **General points**

119. Therefore, when assessing the risk that is likely to result from a breach, the controller should consider a combination of the severity of the potential impact on the rights and freedoms of individuals and the likelihood of these occurring. Clearly, where the consequences of a breach are more severe, the risk is higher and similarly where the likelihood of these occurring is greater, the risk is also heightened. If in doubt, the controller should err on the side of caution and notify. Annex B provides some useful examples of different types of breaches involving risk or high risk to individuals.

120. The European Union Agency for Network and Information Security (ENISA) has produced recommendations for a methodology of assessing the severity of a breach, which controllers and processors may find useful when designing their breach management response plan<sup>46</sup>.

## V. ACCOUNTABILITY AND RECORD KEEPING

### A. Documenting breaches

121. Regardless of whether or not a breach needs to be notified to the supervisory authority, the controller must keep documentation of all breaches, as Article 33(5) GDPR explains:

*"The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article."*

122. This is linked to the accountability principle of the GDPR, contained in Article 5(2) GDPR. The purpose of recording non-notifiable breaches, as well notifiable breaches, also relates to the controller's obligations under Article 24 GDPR, and the supervisory authority can request to see these records. Controllers are therefore encouraged to establish an internal register of breaches, regardless of whether they are required to notify or not<sup>47</sup>.

123. Whilst it is up to the controller to determine what method and structure to use when documenting a breach, in terms of recordable information there are key elements that should be included in all cases. As is required by Article 33(5) GDPR, the controller needs to record details concerning the breach, which should include its causes, what took place and the personal data affected. It should also include the effects and consequences of the breach, along with the remedial action taken by the controller.

124. The GDPR does not specify a retention period for such documentation. Where such records contain personal data, it will be incumbent on the controller to determine the appropriate period of retention in accordance with the principles in relation to the processing of personal data<sup>48</sup> and to meet a lawful basis for processing<sup>49</sup>. It will need to retain documentation in accordance with Article 33(5)

---

<sup>46</sup> ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches, <https://www.enisa.europa.eu/publications/dbn-severity>

<sup>47</sup> The controller may choose to document breaches as part of its record of processing activities which is maintained pursuant to Article 30 GDPR. A separate register is not required, provided the information relevant to the breach is clearly identifiable as such and can be extracted upon request.

<sup>48</sup> See Article 5 GDPR.

<sup>49</sup> See Article 6 and also Article 9 GDPR.

GDPR insofar as it may be called to provide evidence of compliance with that Article, or with the accountability principle more generally, to the supervisory authority. Clearly, if the records themselves contain no personal data then the storage limitation principle<sup>50</sup> of the GDPR does not apply.

125. In addition to these details, the EDPB recommends that the controller also document its reasoning for the decisions taken in response to a breach. In particular, if a breach is not notified, a justification for that decision should be documented. This should include reasons why the controller considers the breach is unlikely to result in a risk to the rights and freedoms of individuals<sup>51</sup>. Alternatively, if the controller considers that any of the conditions in Article 34(3) GDPR are met, then it should be able to provide appropriate evidence that this is the case.

126. Where the controller does notify a breach to the supervisory authority, but the notification is delayed, the controller must be able to provide reasons for that delay; documentation relating to this could help to demonstrate that the delay in reporting is justified and not excessive.

127. Where the controller communicates a breach to the affected individuals, it should be transparent about the breach and communicate in an effective and timely manner. Accordingly, it would help the controller to demonstrate accountability and compliance by retaining evidence of such communication.

128. To aid compliance with Articles 33 and 34 GDPR, it would be advantageous to both controllers and processors to have a documented notification procedure in place, setting out the process to follow once a breach has been detected, including how to contain, manage and recover the incident, as well as assessing risk, and notifying the breach. In this regard, to show compliance with GDPR it might also be useful to demonstrate that employees have been informed about the existence of such procedures and mechanisms and that they know how to react to breaches.

129. It should be noted that failure to properly document a breach can lead to the supervisory authority exercising its powers under Article 58 GDPR and, or imposing an administrative fine in accordance with Article 83 GDPR.

## B. Role of the Data Protection Officer

130. A controller or processor may have a Data Protection Officer (DPO)<sup>52</sup>, either as required by Article 37 GDPR, or voluntarily as a matter of good practice. Article 39 of the GDPR sets a number of mandatory tasks for the DPO, but does not prevent further tasks being allocated by the controller, if appropriate.

131. Of particular relevance to breach notification, the mandatory tasks of the DPO includes, amongst other duties, providing data protection advice and information to the controller or processor, monitoring compliance with the GDPR, and providing advice in relation to DPIAs. The DPO must also cooperate with the supervisory authority and act as a contact point for the supervisory authority and for data subjects. It should also be noted that, when notifying the breach to the supervisory authority, Article 33(3)(b) GDPR requires the controller to provide the name and contact details of its DPO, or other contact point.

132. In terms of documenting breaches, the controller or processor may wish to obtain the opinion of its DPO as to the structure, the setting up and the administration of this documentation. The DPO could also be additionally tasked with maintaining such records.

133. These factors mean that the DPO should play a key role in assisting the prevention of or preparation for a breach by providing advice and monitoring compliance, as well as during a breach

---

<sup>50</sup> See Article 5(1)(e) GDPR.

<sup>51</sup> See Recital 85 GDPR.

<sup>52</sup> See WP Guidelines on DPOs here: [http://ec.europa.eu/newsroom/just/item-detail.cfm?item\\_id=50083](http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083)

(i.e. when notifying the supervisory authority), and during any subsequent investigation by the supervisory authority. In this light, the EDPB recommends that the DPO is promptly informed about the existence of a breach and is involved throughout the breach management and notification process.

## VI. NOTIFICATION OBLIGATIONS UNDER OTHER LEGAL INSTRUMENTS

134. In addition to, and separate from, the notification and communication of breaches under the GDPR, controllers should also be aware of any requirement to notify security incidents under other associated legislation that may apply to them and whether this may also require them to notify the supervisory authority of a personal data breach at the same time. Such requirements can vary between Member States, but examples of notification requirements in other legal instruments, and how these inter-relate with the GDPR, include the following:

- *Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation)*<sup>53</sup>.

135. Article 19(2) of the eIDAS Regulation requires trust service providers to notify their supervisory body of a breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein. Where applicable—i.e., where such a breach or loss is also a personal data breach under the GDPR—the trust service provider should also notify the supervisory authority.

- *Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)*<sup>54</sup>.

136. Articles 14 and 16 of the NIS Directive require operators of essential services and digital service providers to notify security incidents to their competent authority. As recognised by Recital 63 of NIS<sup>55</sup>, security incidents can often include a compromise of personal data. Whilst NIS requires competent authorities and supervisory authorities to co-operate and exchange information that context, it remains the case that where such incidents are, or become, personal data breaches under the GDPR, those operators and/or providers would be required to notify the supervisory authority separately from the incident notification requirements of NIS.

### Example

A cloud service provider notifying a breach under the NIS Directive may also need to notify a controller, if this includes a personal data breach. Similarly, a trust service provider notifying under eIDAS may also be required to notify the relevant data protection authority in the event of a breach.

- *Directive 2009/136/EC (the Citizens' Rights Directive) and Regulation 611/2013 (the Breach Notification Regulation).*

137. Providers of publicly available electronic communication services within the context of Directive 2002/58/EC<sup>56</sup> must notify breaches to the competent national authorities.

---

<sup>53</sup> See [http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L\\_2014.257.01.0073.01.ENG](http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_2014.257.01.0073.01.ENG)

<sup>54</sup> See [http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\\_2016.194.01.0001.01.ENG](http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_2016.194.01.0001.01.ENG)

<sup>55</sup> Recital 63: “Personal data are in many cases compromised as a result of incidents. In this context, competent authorities and data protection authorities should cooperate and exchange information on all relevant matters to tackle any personal data breaches resulting from incidents.”

<sup>56</sup> On 10 January 2017, the European Commission proposed a Regulation on Privacy and Electronic Communications which will replace Directive 2009/136/EC and remove notification requirements. However, until this proposal is approved by the European Parliament the existing notification requirement remains in

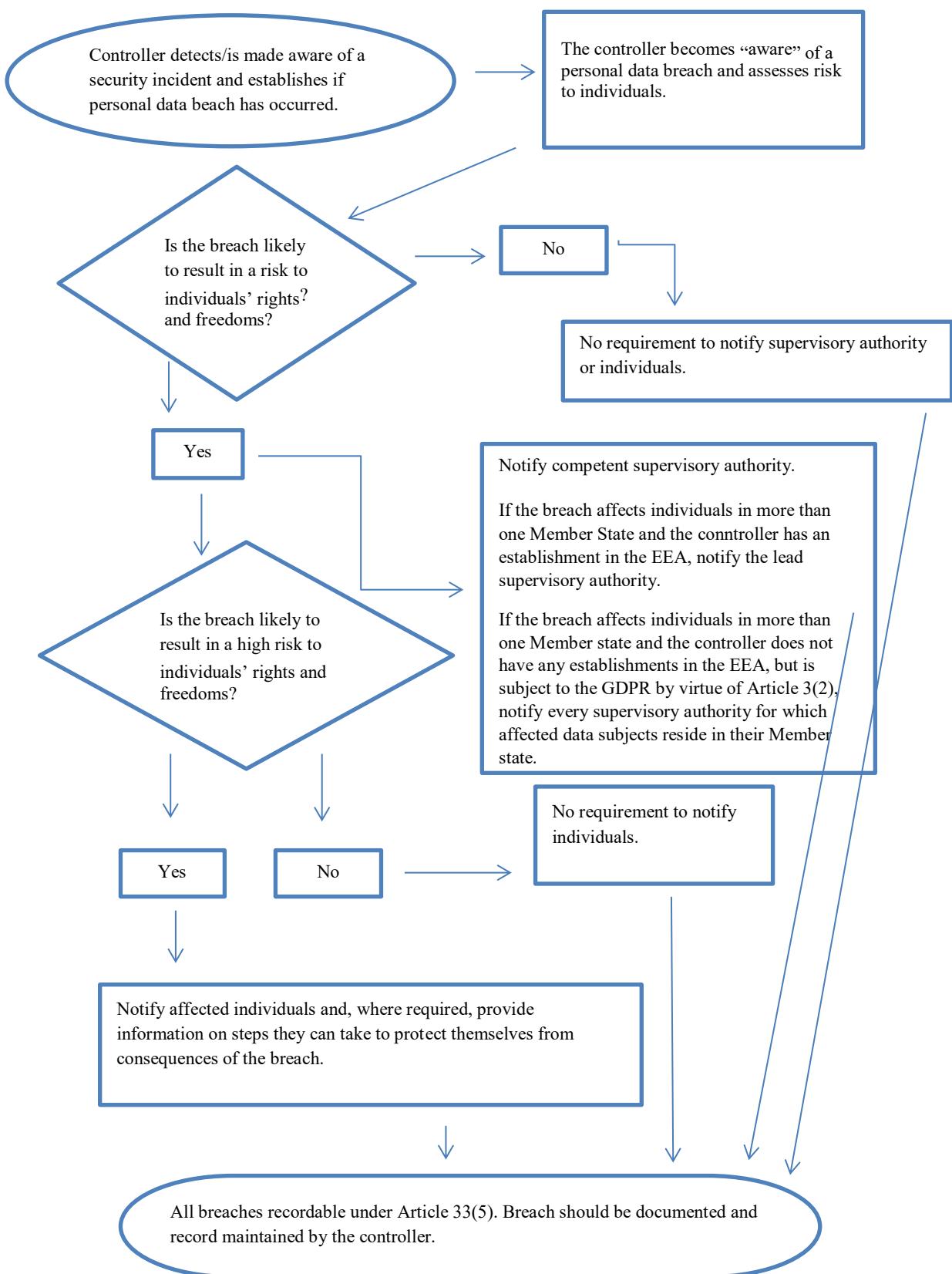
138. Controllers should also be aware of any additional legal, medical, or professional notification duties under other applicable regimes.

---

force, see <https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electroniccommunications>

## VII. ANNEX

### A. Flowchart showing notification requirements



## B. Examples of personal data breaches and who to notify

The following non-exhaustive examples will assist controllers in determining whether they need to notify in different personal data breach scenarios. These examples may also help to distinguish between risk and high risk to the rights and freedoms of individuals.

<b>Example</b>	<b>Notify the supervisory authority</b>	<b>Notify the data subject</b>	<b>Notes/recommendations</b>
i A controller stored a backup of an archive of personal data encrypted on a USB key. The key is stolen during a break-in.	No.	No.	As long as the data are encrypted with a state of the art algorithm, backups of the data exist the unique key is not compromised, and the data can be restored in good time, this may not be a reportable breach. However if it is later compromised, notification is required.
ii A controller maintains an online service. As a result of a cyber attack on that service, personal data of individuals are exfiltrated.  The controller has customers in a single Member State.	Yes, report to the supervisory authority if there are likely consequences to individuals.	Yes, report to individuals depending on the nature of the personal data affected and if the severity of the likely consequences to individuals is high.	
iii A brief power outage lasting several minutes at a controller's call centre meaning customers are unable to call the controller and access their records.	No.	No.	This is not a notifiable breach, but still a recordable incident under Article 33(5). Appropriate records should be maintained by the controller.
iv A controller suffers a ransomware attack which results in all data being encrypted. No backups are available and the data cannot be restored. On investigation, it becomes clear that the ransomware's only functionality	Yes, report to the supervisory authority, if there are likely consequences to individuals as this is a loss of availability.	Yes, report to individuals, depending on the nature of the personal data affected and the possible effect of the lack of availability of the data, as well as other likely consequences.	If there was a backup available and data could be restored in good time, this would not need to be reported to the supervisory authority or to individuals as there would have been no permanent loss of availability or confidentiality. However, if the supervisory authority became aware of the

was to encrypt the data, and that there was no other malware present in the system.			incident by other means, it may consider an investigation to assess compliance with the broader security requirements of Article 32.
---	--	--	--

v An individual phones a bank's call centre to report a data breach. The individual has received a monthly statement for someone else.  The controller undertakes a short investigation (i.e. completed within 24 hours) and establishes with a reasonable confidence that a personal data breach has occurred and whether it has a systemic flaw that may mean other individuals are or might be affected.	Yes.	Only the individuals affected are notified if there is high risk and it is clear that others were not affected.	If, after further investigation, it is identified that more individuals are affected, an update to the supervisory authority must be made and the controller takes the additional step of notifying other individuals if there is high risk to them.
vi A controller operates an online marketplace and has customers in multiple Member States. The marketplace suffers a cyber-attack and usernames, passwords and purchase history are published online by the attacker.	Yes, report to lead supervisory authority if involves cross-border processing.	Yes, as could lead to high risk.	The controller should take action, e.g. by forcing password resets of the affected accounts, as well as other steps to mitigate the risk.  The controller should also consider any other notification obligations, e.g. under the NIS Directive as a digital service provider.
vii A website hosting company acting as a data processor identifies an error in the code which controls user authorisation. The effect of the flaw means that any user	As the processor, the website hosting company must notify its affected clients (the controllers) without undue delay.  Assuming that the website hosting	If there is likely no high risk to the individuals they do not need to be notified.	The website hosting company (processor) must consider any other notification obligations (e.g. under the NIS Directive as a digital service provider).  If there is no evidence of this vulnerability being

	can access the account details of any other user	company has conducted its own investigation the affected controllers should be reasonably confident as to whether each has suffered a breach and therefore is likely to be considered as having “become aware” once they have been notified by the hosting company (the processor). The controller then must notify the supervisory authority		exploited with any of its controllers a notifiable breach may not have occurred but it is likely to be recordable or be a matter of non-compliance under Article 32.
viii	Medical records in a hospital are unavailable for the period of 30 hours due to a cyber-attack.	Yes, the hospital is obliged to notify as high-risk to patient’s well-being and privacy may occur.	Yes, report to the affected individuals.	
ix	Personal data of a large number of students are mistakenly sent to the wrong mailing list with 1000+ recipients.	Yes, report to supervisory authority.	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	
x	A direct marketing e-mail is sent to recipients in the “to:” or “cc:” fields, thereby enabling each recipient to see the email address of other recipients.	Yes, notifying the supervisory authority may be obligatory if a large number of individuals are affected, if sensitive data are revealed (e.g. a mailing list of a psychotherapist) or if other factors present high risks (e.g. the mail contains the initial passwords).	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	Notification may not be necessary if no sensitive data is revealed and if only a minor number of email addresses are revealed.

# Guidelines



## **Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive**

**Version 2.0**

**Adopted on 7 October 2024**

### *Version History*

Version 1.0	14 November 2023	Adoption of the Guidelines for public consultation
Version 2.0	7 October 2024	Adoption of the Guidelines after public consultation

## **Executive summary**

In these Guidelines, the EDPB addresses the applicability of Article 5(3) of the ePrivacy Directive to different technical solutions. These Guidelines expand upon the Opinion 9/2014 of the Article 29 Working Party on the application of ePrivacy Directive to device fingerprinting and aim to provide a clear understanding of the technical operations covered by Article 5(3) of the ePrivacy Directive.

The emergence of new tracking methods to both replace existing tracking tools (for example, cookies, due to discontinued support for third-party cookies by some browser vendors) and create new business models has become a critical data protection concern. While the applicability of Article 5(3) of the ePrivacy Directive is well established and implemented for some tracking technologies such as cookies, there is a need to address ambiguities related to the application of the said provision to emerging tracking tools.

The Guidelines identify three key elements for the applicability of Article 5(3) of the ePrivacy Directive (section 2.1), namely ‘information’, ‘terminal equipment of a subscriber or user’ and ‘gaining access and ‘storage of information and stored information’. The Guidelines further provide a detailed analysis of each element (section 2.2-2.6).

In section 3, that analysis is applied to a non-exhaustive list of use cases representing common techniques, namely:

- URL and pixel tracking
- Local processing
- Tracking based on IP only
- Intermittent and mediated Internet of Things (IoT) reporting
- Unique Identifier

## Table of contents

1	Introduction .....	5
2	Analysis.....	6
2.1	Key elements for the applicability of Article 5(3) ePD .....	6
2.2	Notion of 'information' - Criterion A.....	6
2.3	Notion of 'terminal equipment of a subscriber or user' – Criterion B.1.....	7
2.4	Notion of 'public communications network' – Criterion B.2.....	8
2.5	Notion of 'gaining access' – Criterion C.1 .....	9
2.6	Notions of storage of information' and 'stored information' – Criterion C.2 .....	11
3	Use cases .....	11
3.1	URL and pixel tracking.....	12
3.2	Local processing .....	13
3.3	Tracking based on IP only.....	13
3.4	Intermittent and mediated IoT reporting .....	14
3.5	Unique Identifier .....	14

# The European Data Protection Board

Having regard to Article 70 (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'),

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<sup>1</sup>,

Having regard to Article 15(3) of the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, as amended by Directive 2009/136/EC (hereinafter, 'ePrivacy Directive' or 'ePD'),

Having regard to Article 12 and Article 22 of its Rules of Procedure,

## HAS ADOPTED THE FOLLOWING GUIDELINES:

### 1 INTRODUCTION

1. According to Article 5(3) ePD, '*the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user*' is only allowed on the basis of consent or necessity for specific purposes set out in that Article. As reminded in Recital 24 of the ePD<sup>2</sup>, the goal of that provision is to protect the users' terminal equipment, as they are part of the private sphere of the users. It results from the wording of the Article, that Article 5(3) ePD does not exclusively apply to cookies, but also to 'similar technologies'. However, there is currently no comprehensive list of the technical operations covered by Article 5(3) ePD.
2. Article 29 Working Party (hereinafter, 'WP29') Opinion 9/2014 on the application of ePrivacy Directive to device fingerprinting (hereinafter, 'WP29 Opinion 9/2014') has already clarified that fingerprinting falls within the technical scope of Article 5(3) ePD<sup>3</sup>, but due to the new advances in technologies further guidance is needed with respect to the tracking techniques currently observed. The technical landscape has been evolving during the last decade, with the increasing use of identifiers embedded in operating systems, as well as the creation of new tools allowing the storage of information in terminal equipment.

---

<sup>1</sup> References to 'Member States' made throughout this document should be understood as references to 'EEA Member States'.

<sup>2</sup> 'Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms. So-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned.'

<sup>3</sup> WP29 Opinion 9/2014, p. 11.

3. The ambiguities regarding the scope of application of Article 5(3) ePD have created incentives to implement alternative solutions for tracking internet users and lead to a tendency to circumvent the legal obligations provided by Article 5(3) ePD. All such situations raise concerns and require a supplementary analysis in order to complement the previous guidance from the EDPB.
4. The aim of these Guidelines is to conduct a technical analysis on the scope of application of Article 5(3) ePD, namely to clarify what is technically covered by the phrase '*to store information or to gain access to information stored in the terminal equipment of a subscriber or user*'. These Guidelines do not address the circumstances under which a processing operation may fall within the exemptions from the consent requirement provided for by the ePD<sup>4</sup>, as these circumstances should be analysed on a case-by-case basis accounting for the relevant member state transposition(s), and guidance issued by national Competent Authorities.
5. A non-exhaustive list of specific use-cases will be analysed in the final part of these Guidelines.

## 2 ANALYSIS

### 2.1 Key elements for the applicability of Article 5(3) ePD

6. Article 5(3) ePD applies if:
  - a. **CRITERION A:** the operations carried out relate to '*information*'. It should be noted that the term used is not '*personal data*', but '*information*'.
  - b. **CRITERION B:** the operations carried out involve a '*terminal equipment*' of a subscriber or user (B.1), which imply the need to assess the notion of a '*public communications network*' (B.2).
  - c. **CRITERION C** the operations carried out indeed constitute '*storage*' (C.1) or a '*gaining of access*' (C.2). Those two notions can be studied independently, as reminded in WP29 Opinion 9/2014: '*Use of the words "stored or accessed" indicates that the storage and access do not need to occur within the same communication and do not need to be performed by the same party*'<sup>5</sup>.

For the sake of readability, the entity gaining access to information stored in the user's terminal equipment will be hereafter referred to as an '*accessing entity*'.

### 2.2 Notion of '*information*' - Criterion A

7. As expressed in CRITERION A, this section details what is covered by the notion of '*information*'. The choice of the term '*information*', encompassing a broader category than the mere notion of personal data, is related to the scope of the ePrivacy Directive.
8. The goal of Article 5(3) ePD is to protect the private sphere of the users, as stated in its Recital 24: '*Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European*

---

<sup>4</sup> As stated in Article 5(3) ePD: '*This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.*'

<sup>5</sup> WP29 Opinion 9/2014, p. 8.

*Convention for the Protection of Human Rights and Fundamental Freedoms*'. It is also protected by Article 7 of the EU Charter of Fundamental Rights.

9. In fact, scenarios that do intrude into this private sphere even without involving any personal data are explicitly covered by the wording of Article 5(3) and Recital 24 ePD, for example the storage of viruses on the user's terminal equipment. This shows that the definition of the term 'information' should not be limited to the property of being related to an identified or identifiable natural person.
10. This has been confirmed by the Court of Justice of the EU: '*That protection applies to any information stored in such terminal equipment, regardless of whether or not it is personal data, and is intended, in particular, as is clear from that recital, to protect users from the risk that hidden identifiers and other similar devices enter those users' terminal equipment without their knowledge*'<sup>6</sup>.
11. The questions on whether the origin of this information and the reasons why it is stored in the terminal equipment should be considered when assessing the applicability of Article 5(3) ePD have been previously clarified. For example, in the WP29 Opinion 9/2014: '*It is not correct to interpret this as meaning that the third-party does not require consent to access this information simply because he did not store it. The consent requirement also applies when a read-only value is accessed (e.g. requesting the MAC address of a network interface via the OS API)*'<sup>7</sup>.
12. In conclusion, the notion of information includes both non-personal data and personal data, regardless of how this data was stored and by whom, i.e. whether by an external entity (also including other entities than the one having access), by the user, by a manufacturer, or any other scenario.

### 2.3 Notion of 'terminal equipment of a subscriber or user' – Criterion B.1

13. This section builds on the definition used in Directive 2008/63/EC and as referenced in Article 2 Directive (EU) 2018/1972, where 'terminal equipment' is defined as: '*equipment directly or indirectly connected to the interface of a public telecommunications network to send, process or receive information; in either case (direct or indirect), the connection may be made by wire, optical fibre or electromagnetically; a connection is indirect if equipment is placed between the terminal equipment and the interface of the network*'<sup>8</sup>.
14. Recital 24 ePD provides a clear understanding of the role of the terminal equipment for the protection offered by Article 5(3) ePD. The ePD protects users' privacy not only in relation to the confidentiality of their information but also by safeguarding the integrity of the user's terminal equipment. This understanding will guide the interpretation of the notion of the terminal equipment throughout these Guidelines.
15. Article 3 ePD states that for the ePD to apply the processing of personal data has to be carried out in connection with the provision of publicly available electronic communications services in public communications networks. This entails that a device should be usable in connection with such service and that, in order to be qualified as a terminal equipment, it should be connected or connectable<sup>9</sup> to the interface of a public communications network. The EDPB notes that the amendments made

---

<sup>6</sup> Judgement of the Court of Justice of 1 October 2019, Planet 49, Case C-673/17, ECLI:EU:C:2019:801, paragraph 70.

<sup>7</sup> WP29 Opinion 9/2014, p. 8.

<sup>8</sup> Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment (Codified version), Article 1(1).

<sup>9</sup> That is, having the technical capabilities to be connected to the network even if that connection is not currently in place.

in 2009<sup>10</sup> in the text of Article 5(3) ePD extended the protection of terminal equipment by deleting the reference to the ‘use of electronic communications network’ as a means to store information or to gain access to information stored in the terminal equipment. Therefore, as long as a device has a network interface that makes it eligible for connection (even if such connection is not in place), Article 5(3) ePD applies to every entity that would store and gain access to information already stored in the terminal equipment whatever the means of access to the terminal equipment is, and whether connected or disconnected from a network

16. Equipment that are part of the public electronic communications network itself would not be considered terminal equipment under Article 5(3) ePD<sup>11</sup>.
17. A terminal equipment may be comprised of any number of individual pieces of hardware, which together form the terminal equipment. This may or may not take the form of a physically enclosed device hosting all the display, processing, storage and peripheral hardware (for example, smartphones, laptops, network-attached storage device, connected cars or connected TVs, smart glasses).
18. The ePD acknowledges that the protection of the confidentiality of the information stored on a user’s terminal equipment and integrity of the user’s terminal equipment is not limited to the protection of the private sphere of natural persons but also concerns the right to respect for their correspondence or the legitimate interests of legal persons<sup>12</sup>. As such, a terminal equipment that allows for this correspondence and the legitimate interests of the legal persons to be carried out is protected under Article 5(3) ePD.
19. The user or subscriber may own or rent or otherwise be provided with the terminal equipment. Multiple users or subscribers may share the same terminal equipment.
20. This protection is guaranteed by the ePD to the terminal equipment associated to the user or subscriber, and it is not dependant on whether the user set up the means of access (for example if they initiated the electronic communication) or even on whether the user is aware of the said means of access).

#### 2.4 Notion of ‘public communications network’ – Criterion B.2

21. As the situation regulated by the ePD is the one related to ‘*the provision of publicly available electronic communications services in public communications networks in the Community*’<sup>13</sup>, and the definition of a terminal equipment specifically mentions the notion of a ‘*public communications network*’, it is crucial to clarify this notion to identify the context in which Article 5(3) ePD applies.

---

<sup>10</sup> Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users’ rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance), OJ L 337, 18.12.2009, Article 2(5) and Recital 65.

<sup>11</sup> To identify the limits of the network in different contexts, refer to the BEREC Guidelines on Common Approaches to the Identification of the Network Termination Point in different Network Topologies (BoR (20) 46)

<sup>12</sup> Indeed, as reminded in Art. 2(13) of Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, the user can be a natural or a legal person.

<sup>13</sup> Article 3 ePD.

22. The notion of electronic communications network is not defined within the ePD itself. That concept was referred to originally in Directive 2002/21/EC (the Framework Directive) on a common regulatory framework for electronic communications networks and services<sup>14</sup>, subsequently replaced by Article 2(1) of Directive 2018/1972 (the European Electronic Communications Code). It now reads:

*"electronic communications network" means transmission systems, whether or not based on a permanent infrastructure or centralised administration capacity, and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including internet) and mobile networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed.<sup>15</sup>*

23. This definition is neutral with respect to the transmission technologies. An electronic communications network, according to this definition, is any network system that allows transmission of electronic signals between its nodes, regardless of the equipment and protocols used.
24. The notion of electronic communications network under Directive 2018/1972 does not depend on the public or private nature of the infrastructure, nor on the way the network is deployed or managed ('whether or not based on a permanent infrastructure or centralised administration capacity'<sup>16</sup>.) As a result, the definition of electronic communications network, under Article 2 of Directive 2018/1972, is broad enough to cover any type of infrastructure. It includes networks managed or not by an operator, networks co-managed by a group of operators, or even ad-hoc networks in which a terminal equipment may dynamically join or leave a mesh of other terminal equipment using short range transmission protocols.
25. This definition of network does not give any limitation with regards to the number of terminal equipment present in the network at any time. Some networking schemes rely on nodes relaying information in an ad-hoc manner to nodes presently connected<sup>17</sup> and can at some point in time have as little as two peers communicating. Such cases would be within the general scope of the ePD directive, as long as the network protocol allows for further inclusion of peers.
26. The public availability of the communication network is necessary for the device to be considered a terminal equipment and in consequence for the applicability of Article 5(3) ePD. It should be noted that the fact that the network is made available to a limited subset of the public (for example, subscribers, whether paying or not, subject to eligibility conditions) does not make such a network private<sup>18</sup>.

## 2.5 Notion of 'gaining access' – Criterion C.1

---

<sup>14</sup> 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)

<sup>15</sup> Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast), Text with EEA relevance, Article 2(1).

<sup>16</sup> Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast), Text with EEA relevance, Article 2(1).

<sup>17</sup> For example, in the context of delay-tolerant networking scheme that implement 'store and forward techniques' such as the Briar open source project.

<sup>18</sup> For further analysis on the identification of public communication networks, refer to the BEREC Guidelines on the Implementation of the Open Internet Regulation (BoR (20) 112)

27. To correctly frame the notion of ‘gaining access’, it is important to consider the scope of the ePD, stated in its Article 1: *‘to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community’*.
28. In a nutshell, the ePD is a privacy preserving legal instrument aiming to protect the confidentiality of communications and the integrity of devices. In Recital 24 ePD, it is clarified that, in the case of natural persons, the user’s terminal equipment is part of their private sphere and that accessing information stored on it without their knowledge may seriously intrude upon their privacy.
29. Legal persons are also safeguarded by the ePD<sup>19</sup>. In consequence, the notion of ‘gaining access’ under Article 5(3) ePD, has to be interpreted in a way that safeguards those rights against violation by third parties.
30. Storing information or gaining access can be independent operations, and performed by independent entities. Storing of information and access to information already stored do not need to be both present for Article 5(3) ePD to apply.
31. As noted in the WP29 Opinion 9/2014: *‘Use of the words “stored or accessed” indicates that the storage and access do not need to occur within the same communication and do not need to be performed by the same party. Information that is stored by one party (including information stored by the user or device manufacturer) which is later accessed by another party is therefore within the scope of Art. 5(3)’*<sup>20</sup>. Consequently, there are no restrictions placed on the origin of information on the terminal equipment for the notion of access to apply.
32. Whenever an entity takes steps towards gaining access to information stored in the terminal equipment, Article 5(3) ePD would apply. Usually this entails the accessing entity to proactively send specific instructions to the terminal equipment in order to receive back the targeted information. For example, this is the case for cookies, where the accessing entity instructs the terminal equipment to proactively send information on each subsequent Hypertext Transfer Protocol (‘HTTP’) call.
33. That is equally the case when the accessing entity distributes software on the terminal equipment of the user that is stored and will then proactively call an Application Programming Interface (‘API’) endpoint over the network. Additional examples would include JavaScript code, where the accessing entity instructs the browser of the user to send asynchronous requests with the targeted information. Such access clearly falls within the scope of Article 5(3) ePD, as the accessing entity explicitly instructs the terminal equipment to send the information.
34. In some cases, the entity instructing the terminal equipment to send back the targeted data and the entity receiving information might not be the same. This may result from the provision and/or use of a common mechanism between the two entities. Instructing the device to send already stored information (for example, through the use of a protocol, or an SDK<sup>21</sup> that imply the proactive sending of information by the terminal equipment) makes an intrusion into the terminal equipment possible, therefore such an access triggers the applicability of Article 5(3). ePD. As noted in WP29 Opinion 09/2014, this can be the case when a website instructs the terminal equipment to send information

---

<sup>19</sup> Recital 26 ePD, see paragraph 17 above.

<sup>20</sup> WP29 Opinion 9/2014, p. 8.

<sup>21</sup> An SDK (“software development kit”) is a bundle of software development tools made available to facilitate the creation of application software.

to third-party advertising services through the inclusion of a tracking pixel<sup>22</sup>. This use-case is further developed in section 3.1.

## 2.6 Notions of storage of information' and 'stored information' – Criterion C.2

35. Storage of information in the sense of Article 5(3) ePD refers to placing information on a physical electronic storage medium that is part of a user or subscriber's terminal equipment<sup>23</sup>.
36. Typically, information is not stored in the terminal equipment of a user or subscriber through direct access to the memory of the device by another party, but rather by instructing software on the terminal equipment to generate specific information. Storage taking place through such instructions is considered to be initiated directly by the other party. This includes making use of established protocols such as browser cookie storage as well as customized software, regardless of who created or installed the protocols or software on the terminal equipment.
37. The ePD does not place any upper or lower limit on the length of time that information must persist on a storage medium to be counted as stored, nor is there an upper or lower limit on the amount of information to be stored.
38. Similarly, the notion of storage does not depend on the type of medium on which the information is stored. Typical examples would include hard disc drives ('HDD'), solid state drives ('SSD'), electrically-erasable programmable read-only memory ('EEPROM') and random-access memory ('RAM'), but less typical scenarios involving a medium such as magnetic tape or central processing unit ('CPU') cache are not excluded from the scope of application. The storage medium may be connected internally (e.g. through a SATA connection), externally (e.g. through a USB connection)
39. 'Stored information' refers to information already existing on the terminal equipment, regardless of the source or nature of this information. This includes any result from information storage in the sense of Article 5(3) ePD as described above (either by the same party that would later gain access or by another third party). It furthermore includes results of information storage processes beyond the scope of Article 5(3), ePD, such as: storage on the terminal equipment by the user or subscriber themselves, or by a hardware manufacturer (such as the MAC addresses of network interface controllers), sensors integrated into the terminal equipment or processes and programs executed on the terminal equipment, which may or may not produce information that is dependent on or derived from stored information.

## 3 USE CASES

40. As pointed out in the introduction of these guidelines<sup>24</sup>, they do not analyse the application of the exemptions to the obligation to collect consent provided by Article 5(3) ePD. The EDPB reminds that for all of the cases where there is a storage of information or a gaining of access to information already stored, it would have to be assessed if a consent is needed or whether an exemption under Article 5(3) ePD could apply. The reader should therefore consider the exemptions in their use case, in conjunction with this technical analysis.
41. Without prejudice of the specific context in which those technical categories can be used which are necessary to qualify whether Article 5(3) ePD is applicable, it is possible to identify, in a non-exhaustive

---

<sup>22</sup> WP29 Opinion 9/2014, p. 9.

<sup>23</sup> As defined in section 2.3 of these Guidelines.

<sup>24</sup> See paragraph 4 above.

manner, broad categories of identifiers and information that are widely used and can be subject to the applicability of Article 5(3) ePD.

42. Network communication usually relies on a layered model that necessitates the use of identifiers to allow for a proper establishment and carrying out of the communication. The communication of those identifiers to remote actors is instructed through software following agreed upon communication protocols. As outlined above, the fact that the receiving entity might not be the entity instructing the sending of information does not preclude the application of Article 5(3) ePD. This might concern routing identifiers such as the MAC or IP address of the terminal equipment, but also session identifiers (SSRC, WebSocket identifier), or authentication tokens.
43. In the same manner, the application protocol can include several mechanisms to provide context data (such as HTTP header including ‘accept’ field or user agent), caching mechanism (such as ETag<sup>25</sup>) or other functionalities (cookies being one of them, or HSTS<sup>26</sup>). Once again, relying on those mechanisms to collect information (for example in the context of fingerprinting<sup>27</sup> or the tracking of resource identifiers) can lead to the application of Article 5(3) ePD.
44. On the other hand, there are some contexts in which local applications installed in the terminal equipment uses some information strictly inside the terminal, as it might be the case for smartphone system APIs (access to camera, microphone, GPS sensor, accelerator chip, radio chip, local file access, contact list, identifiers access, etc.). This might also be the case for web browsers that process information stored or generated information inside the device (such as cookies, local storage, WebSQL, or even information provided by the users themselves). The use of such information by an application would not constitute a ‘gaining of access to information already stored’ in the meaning of Article 5(3) ePD as long as the information does not leave the device, but when this information or any derivation of this information is accessed, Article 5(3) ePD would apply.
45. Finally, in some cases malicious software elements are distributed by actors, for example crypto mining software or more generally malware, exploiting the processing abilities of the terminal equipment for the benefit of the distributing actor. The distribution of said malicious software in user’s terminal equipment would constitute a ‘storage’ in the meaning of Article 5(3) ePD. In addition, should the software establish a network connection to send information at a later stage, it would constitute a ‘gaining of access’ in the meaning of Article 5(3) ePD
46. For a subset of these categories that present a specific interest, either because of their widespread usage or because a specific study is warranted with regards to the circumstances of their use, a specific analysis is provided below.

### 3.1 URL and pixel tracking

47. A tracking pixel is a hyperlink to a resource, usually an image file, embedded into a piece of content like a website or an email. This pixel usually fulfils no purpose related to the requested content itself; its sole purpose is to automatically establish a communication by the client to the host of the pixel, which would otherwise not have occurred. This is however not systematic and tracking pixels can also be created by adding additional information to hyperlink loading images that are relevant

---

<sup>25</sup> The HTTP ETag is an identifier that allows to do conditional request based on the validity of the cached client data.

<sup>26</sup> HTTP Strict Transport Security (HSTS) allow servers to specify which resources should always be requested using HTTPS connections.

<sup>27</sup> As noted in the introduction, please see Opinion 9/2014 of the Article 29 Working Party on the application of ePrivacy Directive to device fingerprinting

to the content displayed to the user. Establishment of the communication transmits various information to the host of the pixel, depending on the specific use case.

48. In the case of an email, the sender may include a tracking pixel to detect when the receiver reads the email. Tracking pixels on websites may link to an entity collecting many such requests and thus being able to track users' behaviour. Such tracking pixels may also contain additional identifiers, metadata or content as part of the link. These data points may be added by the owner of the website, possibly related to the user's activity on that website so that analytical usage reports can be generated. They may also be dynamically generated through client-side applicative logic supplied by the entity.
49. Tracking links can function in the same way, but the identifier is appended to the website address. When the Uniform Resource Locator ('URL') is visited by the user, the targeted website loads the requested resource but also collects an identifier which is not relevant in terms of resource identification. They are very commonly used by eCommerce websites to identify the origin of their inbound source of traffic. For example, such websites can provide tracked links to partners to use on their domain so that the e-commerce website knows which of their partners is responsible for a sale and pay a commission, a practice known as affiliate marketing.
50. Both tracking links and tracking pixels can be distributed through a wide variety of channels, for example through emails, websites, or even, in the case of tracking links, through any kind of text messaging systems. That distribution to the user's terminal equipment does constitute storage, at the very least through the caching mechanism of the client-side software. As such, Article 5(3) ePD is applicable, even if this storage is not permanent.
51. The addition of tracking information to URLs or images (pixels) sent to the user constitutes an instruction to the terminal equipment to send back the targeted information (the specified identifier). In the case of dynamically constructed tracking pixels, it is the distribution of the applicative logic (usually a JavaScript code) that constitutes the instruction. As a consequence, it can be considered that the collection of identifiers provided through such tracking mechanisms constitutes a 'gaining of access' in the meaning of Article 5(3) ePD, thus it applies to that step as well.

### 3.2 Local processing

52. Some technologies rely on local processing instructed by software distributed on users' terminal equipment, where the information produced by the local processing is then made available to selected actors through client-side API. This may for example be the case for an API provided by the web browser, where locally generated results may be accessed remotely.
53. If at any point and for example in the client-side code, the processed information is made available to a third-party, for example sent back over the network to a server, such an operation (instructed by the entity producing the client-side code distributed on the user terminal equipment) would constitute a 'gaining of access to information already stored'. The fact that this information is being produced locally does not preclude the application of Article 5(3) ePD.

### 3.3 Tracking based on IP only

- 54. Some providers are developing solutions that only rely on the collection of one component, namely the IP address, in order to track the navigation<sup>28</sup> of the user, in some case across multiple domains. In that context Article 5(3) ePD could apply even though the instruction to make the IP available has been made by a different entity than the receiving one.
- 55. However, gaining access to IP addresses would only trigger the application of Article 5(3) ePD in cases where this information originates from the terminal equipment of a subscriber or user. While it is not systematically the case (for example when CGNAT<sup>29</sup> is activated), the static outbound IPv4 originating from a user's router would fall within that case, as well as IPV6 addresses since they are partly defined by the host. Unless the entity can ensure that the IP address does not originate from the terminal equipment of a user or subscriber, it has to take all the steps pursuant to the Article 5(3) ePD.
- 56. While the present guidelines do not analyse the application of the exemptions to the obligation to collect consent provided by Article 5(3) ePD, it is important to once again recall that the applicability of this article does not systematically mean that consent needs to be collected. The EDPB thus reminds that in each case it would have to be assessed if a consent is needed or whether an exemption under Article 5(3) ePD could apply<sup>30</sup>.

### 3.4 Intermittent and mediated IoT reporting

- 57. IoT (Internet of Things) devices produce information continuously over time, for example through sensors embedded in the device, which may or may not be locally pre-processed. In many cases, information is made available to a remote server, but the modalities of that collection can vary.
- 58. Some IoT devices have a direct connection to a public communication network with a cellular SIM card. Other may have an indirect connection to a public communication network, for example through the use of WIFI or the relay of information to another device through a point-to-point connection (for example, through Bluetooth). The other device can for example be a smartphone or a dedicated gateway which may or may not pre-process the information before sending it to the server.
- 59. IoT devices might be instructed by the manufacturer to always stream the collected information, yet still locally cache the information first, for example until a connection is available.
- 60. In any case the IoT device, where it is connected (directly or indirectly) to a public communications network, would itself be considered a terminal equipment. The fact that the information is streamed or cached for intermittent reporting does not change the nature of that information. In both situations Article 5(3) ePD would apply as there is, through the instruction of code on the IoT device to send the dynamically stored data to the remote server, a 'gaining of access'.

### 3.5 Unique Identifier

- 61. A common tool used by companies is the notion of 'unique identifiers' or 'persistent identifiers'. Such identifiers can be derived from persistent personal data (name and surname, email, phone number, etc.), that is hashed on the user's device, collected and shared amongst several controllers to uniquely identify a person over different datasets (usage data collected through the use of website

---

<sup>28</sup> This is additional to and independent of the use and function of an IP address for the establishment and conveyance or transmission of underlying technical communications, or the fact that it may or may not be personal data (in respect of ePrivacy analysis, it is "information")

<sup>29</sup> Carrier-grade NAT or CGNAT is used by Internet service providers to maximise the use of limited IP address space. It groups a number of subscribers under the same public IP address.

<sup>30</sup> WP29 Opinion 9/2014 provides for some examples when consent might not be needed.

or application, customer relation management (CRM) data related to online or offline purchase or subscription, etc.). On websites, the persistent personal data is generally obtained in the context of authentication or the subscription to newsletters.

62. As outlined before, the fact that information is being entered by the user would not preclude the application of Article 5(3) ePD with regards to storage, as this information is stored temporarily on the terminal equipment before being collected.
63. In the context of ‘unique identifier’ collection on websites or mobile applications, the entity collecting is instructing the browser (through the distribution of client-side code) to send that information. As such a ‘gaining of access’ is taking place and Article 5(3) ePD applies.

# Guidelines



## **Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement**

**Version 2.0**

**Adopted on 26 April 2023**

## Version history

Version 1.0	12 May 2022	Adoption of the Guidelines for public consultation
Version 2.0	26 April 2023	Adoption of the Guidelines after public consultation

## Table of content

Executive summary .....	5
1 Introduction.....	8
2 Technology .....	9
2.1 One biometric technology, two distinct functions .....	9
2.2 A wide variety of purposes and applications .....	10
2.3 Reliability, accuracy and risks for data subjects .....	12
3 Applicable legal framework .....	13
3.1 General legal framework – The EU Charter of Fundamental Rights and the European Convention on Human Rights (ECHR).....	14
3.1.1 Applicability of the Charter.....	14
3.1.2 Interference with the rights laid down in the Charter.....	14
3.1.3 Justification for the interference.....	15
3.2 Specific legal framework – the Law Enforcement Directive.....	19
3.2.1 Processing of special categories of data for law enforcement purposes .....	20
3.2.2 Automated individual decision-making, including profiling .....	22
3.2.3 Categories of the data subjects .....	23
3.2.4 Rights of the data subject.....	23
3.2.5 Other legal requirements and safeguards .....	26
4 Conclusion .....	29
5 Annexes.....	29
Annex I - Template for description of scenarios .....	31
Annex II- Practical guidance for managing FRT projects in LEAs.....	33
1. ROLES AND RESPONSIBILITIES.....	33
2. INCEPTION/BEFORE PROCURING THE FRT SYSTEM.....	34
3. DURING PROCUREMENT AND BEFORE DEPLOYMENT OF THE FRT .....	36
4. RECOMMENDATIONS AFTER DEPLOYMENT OF THE FRT.....	37
Annex III - PRACTICAL EXAMPLES.....	39
1 Scenario 1.....	39
1.1. Description.....	39
1.2. Applicable legal framework.....	40
1.3. Necessity and proportionality - purpose/seriousness of crime .....	40
1.4. Conclusion .....	41
2 Scenario 2.....	41
2.1. Description.....	41

2.2.	Applicable legal framework.....	42
2.3.	Necessity and proportionality - purpose/seriousness of crime/number of persons not involved but affected by processing.....	42
2.4.	Conclusion .....	43
3	Scenario 3.....	43
3.1.	Description.....	43
3.2.	Applicable legal framework.....	44
3.3.	Necessity and proportionality .....	44
3.4.	Conclusion .....	45
4	Scenario 4.....	46
4.1.	Description.....	46
4.2.	Applicable legal framework.....	46
4.3.	Necessity and proportionality .....	47
4.4.	Conclusion .....	47
5	Scenario 5.....	47
5.1.	Description.....	47
5.2.	Applicable legal framework.....	48
5.3.	Necessity and proportionality .....	48
5.4.	Conclusion .....	51
6	Scenario 6.....	51
6.1.	Description.....	51
6.2.	Applicable legal framework.....	52
6.3.	Necessity and proportionality .....	52
6.4.	Conclusion .....	52

## EXECUTIVE SUMMARY

More and more law enforcement authorities (LEAs) apply or intend to apply facial recognition technology (FRT). It may be used to **authenticate** or to **identify** a person and can be applied on videos (e.g. CCTV) or photographs. It may be used for various purposes, including to search for persons in police watch lists or to monitor a person's movements in the public space.

FRT is built on the processing of **biometric data**, therefore, it encompasses the processing of special categories of personal data. Often, FRT uses components of **artificial intelligence** (AI) or machine learning (ML). While this enables large scale data processing, it also induces the risk of discrimination and false results. FRT may be used in controlled 1:1 situations, but also on huge crowds and important transport hubs.

FRT is a **sensitive tool for LEAs**. LEAs are executive authorities and have sovereign powers. FRT is prone to interfere with fundamental rights – also beyond the right to protection of personal data – and is able to affect our social and democratic political stability.

For personal data protection in the law enforcement context, the **requirements of the LED** have to be met. A certain framework regarding the use of FRT is provided for in the LED, in particular Article 3(13) LED (term "biometric data"), Article 4 (principles relating to processing of personal data), Article 8 (lawfulness of processing), Article 10 (processing of special categories of personal data) and Article 11 LED (automated individual decision-making).

Several other fundamental rights may be affected by the application of FRT as well. Hence, the **EU Charter of Fundamental Rights** ("the Charter") is essential for the interpretation of the LED, in particular the right to protection of personal data of Article 8 of the Charter, but also the right to privacy laid down in Article 7 of the Charter.

**Legislative measures** that serve as a legal basis for the processing of personal data directly interfere with the rights guaranteed by Articles 7 and 8 of the Charter. The processing of biometric data under all circumstances constitutes a serious interference in itself. This does not depend on the outcome, e.g. a positive matching. Any limitation to the exercise of fundamental rights and freedoms must be provided for by law and respect the essence of those rights and freedoms.

The legal basis must be **sufficiently clear** in its terms to give citizens an adequate indication of conditions and circumstances in which authorities are empowered to resort to any measures of collection of data and secret surveillance. A mere transposition into domestic law of the general clause in Article 10 LED would lack precision and foreseeability.

Before the national legislator creates a new legal basis for any form of processing of biometric data using facial recognition, the competent data protection supervisory authority should be **consulted**.

Legislative measures have to be **appropriate** for attaining the legitimate objectives pursued by the legislation at issue. An **objective of general interest** – however fundamental it may be – does not, in itself, justify a limitation to a fundamental right. Legislative measures should **differentiate** and target those persons covered by it in the light of the objective, e.g. fighting specific serious crime. If the measure covers all persons in a general manner without such differentiation, limitation or exception, it intensifies the interference. It also intensifies the interference if the data processing covers a significant part of the population.

The data has to be processed in a way that ensures the applicability and effectiveness of the EU data protection rules and principles. Based on each situation, the **assessment of necessity and proportionality** has to also identify and consider all possible implications for other fundamental rights. If the data is systematically processed without the knowledge of the data subjects, it is likely to generate a **general feeling of constant surveillance**. This may lead to chilling effects in regard of some or all of the fundamental rights concerned, such as human dignity under Article 1 of the Charter, freedom of thought, conscience and religion under Article 10 of the Charter, freedom of expression under Article 11 of the Charter as well as freedom of assembly and association under Article 12 of the Charter.

Processing of special categories of data, such as biometric data can only be regarded as "**strictly necessary**" (Art. 10 LED) if the interference to the protection of personal data and its restrictions is limited to what is absolutely necessary, i.e. indispensable, and excluding any processing of a general or systematic nature.

The fact that a photograph has been **manifestly made public** (Art. 10 LED) by the data subject does not entail that the related biometric data, which can be retrieved from the photograph by specific technical means, is considered as having been manifestly made public. Default settings of a service, e.g. making templates publicly available, or absence of choice, e.g. templates are made public without the user being able to change this setting, should not in any way be construed as data manifestly made public.

Article 11 LED establishes a framework for **automated individual decision-making**. The use of FRT entails the use of special categories of data and may lead to profiling, depending on the way and purpose FRT is applied for. In any case, in accordance with Union law and Article 11(3) LED, profiling that results in discrimination against natural persons on the basis of special categories of personal data shall be prohibited.

Article 6 LED regards the necessity to **distinguish between different categories of data subjects**. With regard to data subjects for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with the legitimate aim according to the LED, there is most likely no justification of an interference.

The **data minimisation principle** (Art. 4(1)(e) LED) also requires that any video material not relevant to the purpose of the processing should always be removed or anonymised (e.g. by blurring with no retroactive ability to recover the data) before deployment.

The controller must carefully consider how to (or if it can) meet the requirements for **data subject's rights** before any FRT processing is launched since FRT often involves processing of special categories of personal data without any apparent interaction with the data subject.

The effective exercise of data subject's rights is dependent on the controller fulfilling its **information obligations** (Art. 13 LED). When assessing whether a "specific case" according to Article 13(2) LED exists, several factors need to be taken into consideration, including if personal data is collected without the knowledge of the data subject as this would be the only way to enable data subjects to effectively exercise their rights. Should decision-making be done solely based on FRT, then the data subjects need to be informed about the features of the automated decision making.

As regards **access requests**, when biometric data is stored and connected to an identity also by alpha-numerical data, in line with the principle of data minimization, this should allow for the competent authority to give confirmation to an access request based on a search by those alpha-numerical data

and without launching any further processing of biometric data of others (i.e. by searching with FRT in a database).

The risks for the data subjects are particularly serious if inaccurate data is stored in a police database and/or shared with other entities. The controller must **correct** stored data and FRT systems accordingly (see also recital 47 LED).

The right to **restriction** becomes especially important when it comes to facial recognition technology (based on algorithm(s) and thereby never showing a definitive result) in situations where large quantities of data are gathered and the accuracy and quality of the identification may vary.

A **data protection impact assessment (DPIA)** before the use of FRT is a mandatory requirement, cf. Article 27 LED. The EDPB recommends making public the results of such assessments, or at least the main findings and conclusions of the DPIA, as a trust and transparency enhancing measure.

Most cases of deployment and use of FRT contain intrinsic high risk to the rights and freedoms of data subjects. Therefore, the authority deploying the FRT should **consult** the competent supervisory authority prior to the deployment of the system.

Given the unique nature of biometric data, the authority, implementing and/or using FRT should pay special attention to the **security of processing**, in line with Article 29 LED. In particular, the law enforcement authority should ensure that the system complies with the relevant standards and implements biometric template protection measures. Data protection principles and safeguards must be embedded in the technology before the start of the processing of personal data. Therefore, even when a LEA intends to apply and use FRT from external providers, it has to ensure, e.g. through the procurement procedure, that only FRT built upon the principles of **data protection by design and by default** are deployed.

**Logging** (cf. Art. 25 LED) is an important safeguard for verification of the lawfulness of the processing, both internally (i.e. self-monitoring by the concerned controller/processor) and by external supervisory authorities. In the context of facial recognition systems, logging is recommended also for changes of the reference database and for identification or verification attempts including user, outcome and confidence score. Logging, however, is just one essential element of the overall **principle of accountability** (cf. Art. 4(4) LED). The controller has to be able to demonstrate the compliance of the processing with the basic data protection principles of Article 4(1)-(3) LED.

The EDPB recalls its and the EDPS' joint **call for a ban** of certain kinds of processing in relation to (1) remote biometric identification of individuals in publicly accessible spaces, (2) AI-supported facial recognition systems categorising individuals based on their biometrics into clusters according to ethnicity, gender, as well as political or sexual orientation or other grounds for discrimination (3) use of facial recognition or similar technologies, to infer emotions of a natural person and (4) processing of personal data in a law enforcement context that would rely on a database populated by collection of personal data on a mass-scale and in an indiscriminate way, e.g. by "scraping" photographs and facial pictures accessible online.

A central safeguard to the fundamental rights at stake is **effective supervision** by the competent data protection supervisory authorities. Therefore, Member States have to ensure that the resources of the supervisory authorities are appropriate and sufficient to allow them to fulfil their mandate.

These **guidelines address** law makers at EU and national level, as well as LEAs and their officers implementing and using FRT-systems. Individuals are addressed as far as they are interested generally or as data subjects, in particular as regards data subjects' rights.

The **guidelines intend** to inform about certain properties of FRT and the applicable legal framework in the context of law enforcement (in particular the LED).

- In addition, they provide a **tool to support a first classification of the sensitivity of a given use case** (Annex I).
- They also contain **practical guidance for LEAs that wish to procure and run a FRT-system** (Annex II).
- The guidelines also depict several typical **use cases and list numerous considerations relevant**, especially with regard to the necessity and proportionality test (Annex III).

## 1 INTRODUCTION

1. Facial recognition technology (FRT) may be used to automatically recognise individuals based on their face. FRT often is based on artificial intelligence such as machine learning technologies. Applications of FRT are increasingly tested and used in various areas, from individual use to private organisations and public administration use. Law enforcement authorities (LEAs) also expect advantages from the use of FRT. It promises solutions to relatively new challenges such as investigations involving a big amount of captured evidence, but also to known problems, in particular with regard to under-staffing for observation and search tasks.
2. A great deal of the increased interest in FRT is based on the efficiency and scalability of FRT. With these come the disadvantages inherent to the technology and its application – also on a large scale. While there may be thousands of personal data sets analysed at the push of a button, already slight effects of algorithmic discrimination or misidentification may create high numbers of individuals affected severely in their conduct and daily lives. The sheer size of processing of personal data, and in particular biometric data, is a further key element of FRT, as the processing of personal data constitutes an interference with the fundamental right to protection of personal data according to Article 8 of the Charter of Fundamental Rights of the European Union (the Charter).
3. The application of FRT of LEAs will – and to some extent already does – have significant implications on individuals and on groups of people, including minorities. These implications will also have considerable effects on the way we live together and on our social and democratic political stability, valuing the high significance of pluralism and political opposition. The right to protection of personal data often is key as a prerequisite to guarantee other fundamental rights. The application of FRT is considerably prone to interfere with fundamental rights beyond the right to protection of personal data.
4. The EDPB therefore deems it important to contribute to the ongoing integration of FRT in the area of law enforcement covered by the Law Enforcement Directive<sup>1</sup> respectively the national laws transposing it and provide the present guidelines. The guidelines are intended to provide relevant information to lawmakers at EU and national level, as well as for LEAs and their officers when implementing and using FRT-systems. The scope of the guidelines is limited to FRT. However, other forms of processing of personal data based on biometrics by LEAs, especially if processed remotely, may entail similar or additional risks for individuals, groups and society. According to the respective

---

<sup>1</sup> 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.

circumstances, some aspects of these guidelines may serve as a useful source in these cases, as well. Finally, individuals that are interested generally or as data subjects may also find important information, in particular as regards data subjects' rights.

5. The guidelines consist of the main document and three annexes. The main document at hand presents the technology and the legal framework applicable. To help identifying some of the major aspects to classify the severity of the interference with fundamental rights to a given field of application, a template can be found in Annex I. LEAs that wish to procure and run a FRT system may find practical guidance in Annex II. Depending on the field of application of FRT, different considerations could be of relevance. A set of hypothetical scenarios and relevant considerations may be found in Annex III.

## 2 TECHNOLOGY

### 2.1 One biometric technology, two distinct functions

6. Facial recognition is a probabilistic technology that can automatically recognise individuals based on their face in order to authenticate or identify them.
7. FRT falls into the broader category of biometric technology. Biometrics include all automated processes used to recognise an individual by quantifying physical, physiological or behavioural characteristics (fingerprints, iris structure, voice, gait, blood vessel patterns, etc.). These characteristics are defined as "biometric data", because they allow or confirm the unique identification of that person.
8. This is the case with people's faces or, more specifically, their technical processing using facial recognition devices: by taking the image of a face (a photograph or video) called a biometric "sample", it is possible to extract a digital representation of distinct characteristics of this face (this is called a "template").
9. A biometric template is a digital representation of the unique features that have been extracted from a biometric sample and can be stored in a biometric database<sup>2</sup>. This template is supposed to be unique and specific to each person and it is, in principle, permanent over time<sup>3</sup>. In the recognition phase, the device compares this template with other templates previously produced or calculated directly from biometric samples such as faces found on an image, photo or video. "Facial recognition" is therefore a two-step process: the collection of the facial image and its transformation into a template, followed by the recognition of this face by comparing the corresponding template with one or more other templates.
10. Like any biometric process, facial recognition can fulfil two distinct functions:
  - the **authentication** of a person, aimed at verifying that a person is who she or he claims to be. In this case, the system will compare a pre-recorded biometric template or sample (e.g. stored on a smartcard or biometric passport) with a single face, such as that of a person turning up at a checkpoint, in order to verify whether this is one and the same person. This functionality therefore relies on the comparison of two templates. This is also called **1-to-1 verification**.
  - the **identification** of a person, aimed at finding a person among a group of individuals, within a specific area, an image or a database. In this case, the system must process each face captured, to generate a biometric template and then check whether it matches with a person known to the

---

<sup>2</sup> Guidelines on facial recognition, Consultative Committee of Convention 108 the Convention for the protection of individuals with regard to automatic processing of personal data, Council of Europe, June 2021.

<sup>3</sup> This might depend on the type of biometry and the age of the data subject.

system. This functionality thus relies on comparing one template with a database of templates or samples (baseline). This is also called 1-to-many identification. For example, it can link a personal name record (surname, first name) to a face, if the comparison is made against a database of photographs associated with surnames and first names. It can also involve following a person through a crowd, without necessarily making the link with the person's civil identity.

11. In both cases, the used facial recognition techniques are based on an estimated match between templates: the one being compared and the baseline(s). From this point of view, they are probabilistic: the comparison deduces a higher or lower probability that the person is indeed the person to be authenticated or identified; if this probability exceeds a certain threshold in the system, defined by the user or the developer of the system, the system will assume that there is a match.
12. While both functions – authentication and identification – are distinct, they both relate to the processing of biometric data related to an identified or identifiable natural person and therefore constitute a processing of personal data, and more specifically a processing of special categories of personal data.
13. Facial recognition is part of a wider spectrum of video image processing techniques. Some video cameras can film people within a defined area, in particular their faces, but they cannot be used as such to automatically recognise individuals. The same applies to simple photography: a camera is not a facial recognition system because photographs of people need to be processed in a specific way in order to extract biometric data.
14. The mere detection of faces by so-called "smart" cameras does not necessarily constitute a facial recognition system either. While they also raise important questions in terms of ethics and effectiveness, digital techniques for detecting abnormal behaviours or violent events, or for recognising facial emotions or even silhouettes, they may not be considered as biometric systems processing special categories of personal data, provided that they do not aim at uniquely identifying a person and that the personal data processing involved does not include other special categories of personal data. These examples are not completely unrelated to facial recognition and are still subject to personal data protection rules.<sup>4</sup> Furthermore, this type of detection system may be used in conjunction with other systems aiming at identifying a person and thereby being considered as a facial recognition technology.
15. Unlike video capture and processing systems, for example, which require the installation of physical devices, facial recognition is a software functionality which can be implemented within existing systems (cameras, image databases, etc.). Such functionality can therefore be connected or interfaced with a multitude of systems, and combined with other functionalities. Such integration into an already existing infrastructure requires specific attention because it comes with inherent risks due to the fact that the facial recognition technology could be frictionless and easily hidden<sup>5</sup>.

## 2.2 A wide variety of purposes and applications

16. Beyond the scope of these guidelines and outside the scope of the LED, facial recognition may be used for a wide variety of objectives, both for commercial use and for addressing public safety or law enforcement concerns. It may be applied in many different contexts: in the personal relationship between a user and a service (access to an application), for access to a specific place (physical filtering),

---

<sup>4</sup> Article 10 LED (or Article 9 GDPR) is applicable, however, to systems that are used to categorise individuals based on their biometrics into clusters according to ethnicity as well as political or sexual orientation or other special categories of personal data.

<sup>5</sup> For instance, in body-worn cameras which are increasingly being used in practice.

or without any particular limitation in the public space (live facial recognition). It can be applied to any kind of data subject: a customer of a service, an employee, a simple onlooker, a wanted person or someone implicated in legal or administrative proceedings, etc. Some uses are already commonplace and widespread; others are, at this point, at the experimental or speculative stage. While these guidelines will not be addressing all such uses and applications, the EDPB recalls that they may only be implemented if compliant with the applicable legal framework, and in particular with the GDPR and relevant national laws.<sup>6</sup> Even in the context of the LED, further to the functions of authentication or identification, data processed with the use of facial recognition technology can also be further processed for other purposes, such as categorisation.

17. More specifically, a scale of potential uses might be considered depending on the degree of control people have over their personal data, the effective means they have for exercising such control and their right to initiative to trigger and use of this technology, the consequences for them (in the case of recognition or non-recognition) and the scale of the processing carried out. Facial recognition based on a template stored on a personal device (smartcard, smartphone, etc.) belonging to that person, used for authentication and of strictly personal use through a dedicated interface, does not pose the same risks as, for example, usage for identification purposes, in an uncontrolled environment, without the active involvement of the data subjects, where the template of each face entering the monitoring area is compared with templates from a broad cross-section of the population stored in a database. Between these two extremes lies a very varied spectrum of uses and associated issues related to the protection of personal data.
18. In order to further illustrate the context within which facial recognition technologies are currently being debated or implemented, either for authentication or identification, the EDPB deems relevant to mention a series of examples. The examples below are solely descriptive and should not be considered as any kind of preliminary assessment of their compliance with the EU acquis in the field of data protection.

*Examples of facial recognition authentication*

19. Authentication can be designed for users to have full control over it, for example to enable access to services or applications purely within a home setting. As such, it is used extensively by smartphone owners to unlock their device, instead of password authentication.
20. Facial recognition authentication may also be used to check the identity of someone hoping to benefit from public or private third-party services. Such processes thus offer a way of creating a digital identity using a mobile app (smartphone, tablet, etc.) which can then be used to access online administrative services.
21. Furthermore, facial recognition authentication can aim at controlling physical access to one or more predetermined locations, such as entrances to buildings or specific crossing points. This functionality is, for example, implemented in certain processing for the purpose of border crossing, where the face of the person at the checkpoint device is compared with the one stored in their identity document (passport or secure residence permit).

*Examples of facial recognition identification*

---

<sup>6</sup> See also EDPB guidelines 3/2019 on processing of personal data through video devices adopted on 29 January 2020, for further guidance.

22. Identification may be applied in many, even more diverse ways. These particularly include, but are not limited to, the uses listed below, currently observed, experimented or planned in the EU.
- searching, in a database of photographs, for the identity of an unidentified person (victim, suspect, etc.);
  - monitoring of a person's movements in the public space. His or her face is compared with the biometric templates of people travelling or having travelled in the monitored area, for example when a piece of luggage is left behind or after a crime has been committed;
  - reconstructing a person's journey and their subsequent interactions with other persons, through a delayed comparison of the same elements in a bid to identify their contacts for example;
  - remote biometric identification of wanted persons in public spaces. All faces captured live by video-protection cameras are cross-checked, in real time, against a database held by the security forces;
  - automatic recognition of people in an image to identify, for example, their relationships on a social network, which uses it. The image is compared with the templates of everyone on the network who has consented to this functionality in order to suggest the nominative identification of these relationships;
  - access to services, with some cash dispensers recognising their customers, by comparing a face captured by a camera with the database of facial images held by the bank;
  - tracking of a passenger's journey at a certain stage of the journey. The template, calculated in real time, of any person checking in at gates located at certain stages of the journey (baggage drop-off points, boarding gates, etc.), is compared with the templates of people previously registered in the system.

23. In addition to the use of FRT in the field of law enforcement, the wide range of applications observed certainly calls for a comprehensive debate and policy approach in order to ensure consistency and compliance with the EU acquis in the field of data protection.

### 2.3 Reliability, accuracy and risks for data subjects

24. Like every technology, facial recognition may also be subject to challenges when it comes to its implementation, in particular when it comes to its reliability and efficiency in terms of authentication or identification, as well as the overall issue of quality and accuracy of the "source" data and the result of facial recognition technology processing.
25. Such technological challenges entail particular risks for data subjects concerned which are all the more significant or serious in the area of law enforcement considering the possible effects for data subjects either legal, or other ones similarly affecting them in a significant manner. In this context, it appears also useful to underline that the ex post use of FRT is not per se safer, as individuals may be tracked across time and places. Thus, the ex post use also poses specific risks which have to be assessed on a case-by-case basis.<sup>7</sup>
26. As pointed out by the EU Fundamental Rights Agency in its 2019 report, "determining the necessary level of accuracy of facial recognition software is challenging: there are many different ways to evaluate and assess accuracy, also depending on the task, purpose and context of its use. When

---

<sup>7</sup> See the examples presented in Annex III.

applying the technology in places visited by millions of people – such as train stations or airports – a relatively small proportion of errors (e.g. 0.01%)<sup>8</sup> still means that hundreds of people are wrongly flagged. In addition, certain categories of people may be more likely to be wrongly matched than others, as described in Section 3. There are different ways to calculate and interpret error rates, so caution is required. In addition, when it comes to accuracy and errors, questions in relation to how easily a system can be tricked by, for example, fake face images (called ‘spoofing’) are important particularly for law enforcement purposes.”<sup>9</sup>

27. In this context, the EDPB considers it important to recall that FRT, whether used for the purposes of authentication or identification, do not provide for a definitive result but rely on probabilities that two faces, or images of faces, correspond to the same person.<sup>10</sup> This result is further degraded when the quality of biometric sample input to the facial recognition is low. Blurriness of input images, low resolution of camera, motion and low light, can be factors of low quality. Other aspects with significant impact on the results are prevalence and spoofing, e.g. when criminals try to either avoid passing by the cameras or to trick the FRT. Numerous studies have also highlighted that such statistical results from algorithmic processing may also be subject to bias, notably resulting from the source data quality as well as training databases, or other factors, like the choice of location of the deployment. Furthermore, one should also highlight the impact of facial recognition technology on other fundamental rights, such as the respect for private and family life, freedom of expression and information, freedom of assembly and association, etc.
28. It is therefore essential that the reliability and accuracy of facial recognition technology is taken into account as criteria for the assessment of compliance with key data protection principles, as per Article 4 LED, and in particular when it comes to fairness and accuracy.
29. While highlighting that high-quality data is essential for high quality algorithms, the EDPB also stresses the need for data controllers, as part of their accountability obligation, to undertake regular and systematic evaluation of algorithmic processing in order to ensure in particular the accuracy, fairness and reliability of the result of such personal data processing. Personal data used for the purposes of evaluating, training and further developing FRT systems may only be processed on the basis of a sufficient legal basis and in accordance with the common data protection principles.

### 3 APPLICABLE LEGAL FRAMEWORK

30. The use of facial recognition technologies is intrinsically linked to processing of personal data, including special categories of data. Moreover, it has direct or indirect impact on a number of fundamental rights, enshrined in the EU Charter of Fundamental Rights. This is particularly relevant in the area of law enforcement and criminal justice. Therefore, any use of facial recognition technologies should be carried out in strict compliance with the applicable legal framework.
31. The following information is intended to be used for consideration when assessing future legislative and administrative measures as well as implementing existing legislation on a case-by-case basis that involves FRT. The relevance of the respective requirements varies according to the particular

---

<sup>8</sup> This accuracy rate stems from the report quoted and reflects a rate much better than the current performance of algorithms in applications of FRT.

<sup>9</sup> Facial recognition technology: fundamental rights considerations in the context of law enforcement, EU Fundamental Right Agency, 21<sup>st</sup> November 2019.

<sup>10</sup> This probability is referred to as “confidence score”.

circumstances. As not all future circumstances may be foreseen, it is only considered to be providing support and not to be interpreted as an exhaustive enumeration.

### 3.1 General legal framework – The EU Charter of Fundamental Rights and the European Convention on Human Rights (ECHR)

#### 3.1.1 Applicability of the Charter

32. The EU Charter of Fundamental Rights (hereinafter “the Charter”) is addressed to the institutions, bodies, offices and agencies of the Union and to the Member States when they are implementing Union law.
33. Regulating the processing of biometric data for law enforcement purposes according to Article 1(1) LED inevitably raises the question of compliance with fundamental rights, in particular the respect for private life and communications under Article 7 of the Charter and the right to protection of personal data under Article 8 of the Charter.
34. The collection and analysis of video footage of natural persons, including their faces, implies the processing of personal data. When technically processing the image, the processing also covers biometric data. The technical processing of data relating to the face of a natural person in relation to time and place allows conclusions to be drawn concerning the private lives of the relevant persons. Those conclusions may refer to the racial or ethnic origins, health, religion, habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them. The great range of the information that may be revealed by the application of FRT clearly shows the possible impact on the right to the protection of personal data laid down in Article 8 of the Charter, but also on the right to privacy laid down in Article 7 of the Charter.
35. In such circumstances it is also not inconceivable that the collection, analysis and further processing of the biometric (facial) data in question might have an effect on the way that people feel free to act even if the act would be fully within the remits of a free and open society. It might also have severe implications on the exercise of their fundamental rights, such as their right to freedom of thought, conscience and religion, expression of peaceful assembly and freedom of association under Articles 1, 10, 11 and 12 of the Charter. Such processing also involves other risks, such as the risk of abuse of the personal information gathered by the relevant authorities as a result of unlawful access to and use of the personal data, security breach etc. The risks often depend on the processing and its circumstances, such as the risk of unlawful access and use by police officers or by other unauthorised parties. However, some risks simply are inherent to the unique nature of biometric data. Unlike an address or a telephone number, it is impossible for a data subject to change his or her unique characteristics, such as the face or the iris. In the case of unauthorised access or accidental publication of biometric data, this would lead to the data being compromised in their use as passwords or cryptographic keys or could be used for further, unauthorised surveillance activities to the detriment of the data subject.

#### 3.1.2 Interference with the rights laid down in the Charter

36. The processing of biometric data under all circumstances constitutes a serious interference in itself. This does not depend on the outcome, e.g. a positive matching. The processing constitutes an interference even if the biometric template is immediately deleted after the matching against a police database results in a no-hit.

- 37. The interference with the fundamental rights of the data subjects may stem from an act of law that either aims at or has the effect of restricting the respective fundamental right<sup>11</sup>. It may also result from an act of a public authority with the same purpose or effect or even of a private entity entrusted by law to exercise public authority and public powers.
- 38. A legislative measure that serves as a legal basis for the processing of personal data directly interferes with the rights guaranteed by Articles 7 and 8 of the Charter<sup>12</sup>.
- 39. The use of biometric data and FRT in particular in many cases also affects the right to human dignity, guaranteed by Article 1 of the Charter. Human dignity requires that individuals are not treated as mere objects. FRT calculates existential and highly personal characteristics, the facial features, into a machine-readable form with the purpose of using it as a human license plate or ID card, thereby objectifying the face.
- 40. Such a processing may also interfere with other fundamental rights, such as the rights under Articles 10, 11 and 12 of the Charter insofar as chilling effects are either intended by or derive from the relevant video surveillance of law enforcement agencies.
- 41. In addition, the potential risks generated by the use of facial recognition technologies by law enforcement with regard to the right to fair trial and the presumption of innocence under Articles 47 and 48 of the Charter should also be carefully considered. The outcome of the application of FRT, e.g. a match, may not only lead to a person being subject to further policing, but also be decisive evidence in court proceedings. Shortcomings of FRT such as possible bias, discrimination or wrong identification ('false positive') may thus lead to severe implications also on criminal proceedings. Furthermore, in the assessment of evidence, the outcome of the application of FRT may be favoured, even if there is contradicting evidence ('automation bias').

### **3.1.3 Justification for the interference**

- 42. According to Article 52(1) of the Charter, any limitation to the exercise of fundamental rights and freedoms must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others.

#### ***3.1.3.1 Provided for by law***

- 43. Article 52(1) of the Charter sets the requirement of a specific legal basis. This legal basis must be sufficiently clear in its terms to give citizens an adequate indication of the conditions and circumstances in which authorities are empowered to resort to any measures of collection of data and secret surveillance<sup>13</sup>. It must indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities so as to ensure individuals the minimum degree of protection as entitled under the rule of law in a democratic society<sup>14</sup>. Moreover, lawfulness requires adequate safeguards to ensure that in particular an individual's right under Article 8 of the Charter is respected. These principles also apply to the processing of personal data for purposes of evaluating, training and further developing of FRT systems.

---

<sup>11</sup> CJEU, C-219/91 – Ter Voort, RoC 1992 I-05485, para. 36f; CJEU, C-200/96 – Metronome, RoC 1998 I-1953, para. 28.

<sup>12</sup> CJEU, C-594/12, para. 36; CJEU, C-291/12, para. 23 and the following.

<sup>13</sup> ECtHR, Shimovolos v. Russia, § 68; Vukota-Bojić v. Switzerland.

<sup>14</sup> ECtHR, Piechowicz v. Poland, § 212.

44. Given that biometric data when processed for the purpose of uniquely identifying a natural person constitute special categories of data listed in Article 10 LED, the different applications of FRT in most cases would require a dedicated law precisely describing the application and the conditions for its use. This encompasses in particular the types of crime and, where applicable, the appropriate threshold of severity of these crimes, in order to, among other things, effectively exclude petty crime.<sup>15</sup>

### *3.1.3.2 The essence of the fundamental right to privacy and to protection of personal data laid down in Articles 7 and 8 of the Charter*

45. The limitations of the fundamental rights imminent to each situation still have to provide for the essence of the particular right to be respected. The essence refers to the very core of the relevant fundamental right<sup>16</sup>. Human dignity has to be respected too, even where a right is restricted<sup>17</sup>.
46. Indications of a possible infringement of the inviolable core are the following:
- A provision that imposes limitations irrespective of a person's individual conduct or exceptional circumstances<sup>18</sup>.
  - The recourse to the courts is not possible or hindered<sup>19</sup>.
  - Prior to a severe limitation, the circumstances of the individual concerned are not taken into account<sup>20</sup>.
  - With a view to the rights under Articles 7 and 8 of the Charter: In addition to a broad collection of communication meta-data, the acquisition of the knowledge of the content of the electronic communication could violate the essence of those rights<sup>21</sup>.
  - With a view to the rights under Articles 7, 8 and 11 of the Charter: Legislation which requires that providers of access to online public communication services and hosting service providers retain, generally and indiscriminately, *inter alia*, personal data relating to those services<sup>22</sup>.
  - With reference to the rights under Article 8 of the Charter: A lack of basic principles of data protection and data security could also infringe the core of the right<sup>23</sup>.

### *3.1.3.3 Legitimate aim*

47. As already explained in point 3.1.3., limitations to the fundamental rights have to genuinely meet objectives of general interest recognised by the European Union or meet the need to protect the rights and freedoms of others.
48. Recognised by the Union are both the objectives mentioned in Article 3 of the Treaty on the European Union and other interests protected by specific provisions of the Treaties<sup>24</sup>, i.e. – *inter alia* – an area of freedom, security and justice, the prevention and combating of crime. In its relations with the wider world, the Union should contribute to peace and security and the protection of human rights.

---

<sup>15</sup> See e.g. CJEU judgments in cases C-817/19 Ligue des droits humains, para. 151 f, C-207/16 Ministerio Fiscal, para. 56.

<sup>16</sup> CJEU C-279/09, RoC 2010 I-13849, para. 60.

<sup>17</sup> Explanations relating to the Charter of Fundamental Rights, Title I, Explanation on Article 1, OJ C 303, 14.12.2007, p. 17–35.

<sup>18</sup> CJEU C-601/15, para 52.

<sup>19</sup> CJEU C-400/10, RoC 2010 I-08965, para. 55.

<sup>20</sup> CJEU C-408/03, RoC 2006 I-02647, para. 68.

<sup>21</sup> CJEU - 203/15 - Tele2 Sverige, para. 101 with reference to CJEU - C-293/12 and C-594/12, para. 39.

<sup>22</sup> CJEU C-512/18, La Quadrature du Net, para. 209 et seq.

<sup>23</sup> CJEU - C-594/12, para. 40.

<sup>24</sup> Explanations relating to the Charter of Fundamental Rights, Title I, Explanation on Article 52, OJ C 303, 14.12.2007, p. 17–35.

49. The need to protect the rights and freedoms of others refers to rights of persons that are protected by the law of the European Union or of its Member States. The assessment must be carried out with the aim to reconcile the requirements of the protection of the respective rights and to strike a fair balance between them<sup>25</sup>.

### *3.1.3.4 Necessity and proportionality test*

50. Where interferences with fundamental rights are at issue, the extent of the national and Union legislator's discretion may prove to be limited. This depends on a number of factors, including the area concerned, the nature of the right in question guaranteed by the Charter, the nature and seriousness of the interference and the objective pursued by the interference<sup>26</sup>. Legislative measures have to be appropriate for attaining the legitimate objectives pursued by the legislation at issue. Moreover, the measure must not exceed the limits of what is appropriate and necessary in order to achieve those objectives<sup>27</sup>. An objective of general interest – however fundamental it may be – does not, in itself, justify a limitation to a fundamental right<sup>28</sup>.
51. According to the CJEU's settled case-law, derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary<sup>29</sup>. This also implies that there are no less intrusive means available to achieve the purpose. Possible alternatives such as – depending on the given purpose – additional staffing, more frequent policing or additional street lighting have to be carefully identified and assessed. Legislative measures should differentiate and target those persons covered by it in the light of the objective, e.g. fighting serious crime. If it covers all persons in a general manner without such differentiation, limitation or exception, it intensifies the interference<sup>30</sup>. It also intensifies the interference if the data processing covers a significant part of the population<sup>31</sup>.
52. The protection of personal data resulting from the explicit obligation laid down in Article 8(1) of the Charter is especially important for the right to respect for private life enshrined in Article 7 of the Charter<sup>32</sup>. Legislation must lay down clear and precise rules governing the scope and application of the measure in question and impose safeguards so that the persons whose data have been processed have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access or use of that data<sup>33</sup>. The need for such safeguards is all the greater where personal data is subject to automatic processing and where there is a significant risk of unlawful access to the

---

<sup>25</sup> Jarass GrCh, 3. Aufl. 2016, EU-Grundrechte-Charta Art. 52 Rn. 31-32.

<sup>26</sup> CJEU - C-594/12, para. 47 with the following sources: see, by analogy, as regards Article 8 of the ECHR, Eur. Court H.R., S. and Marper v. the United Kingdom [GC], nos. 30562/04 and 30566/04, § 102, ECHR 2008-V.

<sup>27</sup> CJEU - C-594/12, para. 46 with the following sources: Case C-343/09 Afton Chemical EU:C:2010:419, paragraph 45; Volker und Markus Schecke and Eifert EU:C:2010:662, paragraph 74; Cases C-581/10 and C-629/10 Nelson and Others EU:C:2012:657, paragraph 71; Case C-283/11 Sky Österreich EU:C:2013:28, paragraph 50; and Case C- 101/12 Schaible EU:C:2013:661, paragraph 29.

<sup>28</sup> CJEU - C-594/12, para. 51.

<sup>29</sup> CJEU - C-594/12, para. 52, with the following sources: Case C-473/12 IPI EU:C:2013:715, paragraph 39 and the case-law cited.

<sup>30</sup> CJEU - C-594/12, para. 57.

<sup>31</sup> CJEU - C-594/12, para. 56.

<sup>32</sup> CJEU - C-594/12, para. 53.

<sup>33</sup> CJEU - C-594/12, para. 54, with the following sources: see, by analogy, as regards Article 8 of the ECHR, Eur. Court H.R., Liberty and Others v. the United Kingdom, 1 July 2008, no. 58243/00, § 62 and 63; Rotaru v. Romania, § 57 to 59, and S. and Marper v. the United Kingdom, § 99.

data<sup>34</sup>. Furthermore, internal or external, e.g. judicial, authorisation of the deployment of FRT may also contribute as safeguards, and may prove to be necessary in certain cases of severe interference.<sup>35</sup>

53. The rules laid down have to be adapted to the specific situation, e.g. the quantity of data processed, the nature of the data<sup>36</sup> and the risk of unlawful access to the data. This calls for rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality<sup>37</sup>.
54. With regard to the relationship between the controller and the processor it should not be permitted for the processors to have regard only to economic considerations when determining the level of security which they apply to personal data; this could endanger a sufficient high level of protection<sup>38</sup>.
55. An act of law has to lay down substantive and procedural conditions and objective criteria by which to determine the limits of competent authorities' access to data and their subsequent use. For the purposes of prevention, detection or criminal prosecutions, the offences concerned would have to be considered sufficiently serious to justify the extent and seriousness of these interferences with the fundamental rights enshrined for example in Articles 7 and 8 of the Charter<sup>39</sup>.
56. The data has to be processed in a way that ensures the applicability and effect of the EU data protection rules; in particular those provided by Article 8 of the Charter, which states that the compliance with the requirements of protection and security shall be subject to control by an independent authority. The geographical place where the processing takes place may in such a situation be relevant<sup>40</sup>.
57. With regard to the different steps of processing of personal data, a distinction should be made between the categories of data on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned<sup>41</sup>. The determination of the conditions of the processing, for example, the determination of the retention period, must be based on objective criteria in order to ensure that the interference is limited to what is strictly necessary<sup>42</sup>.
58. Based on each situation, the assessment of necessity and proportionality has to identify and consider all implications that fall within the scope of other fundamental rights, such as human dignity under Article 1 of the Charter, freedom of thought, conscience and religion under Article 10 of the Charter, freedom of expression under Article 11 of the Charter as well as freedom of assembly and association under Article 12 of the Charter.
59. Furthermore, it has to be considered as a matter of severity, that if the data is systematically processed without the knowledge of the data subjects, it is likely to generate a general conception of constant

---

<sup>34</sup> CJEU - C-594/12, para. 55, with the following sources: see, by analogy, as regards Article 8 of the ECHR, S. and Marper v. the United Kingdom, § 103, and M. K. v. France, 18 April 2013, no. 19522/09, § 35.

<sup>35</sup> ECtHR, Szabó and Vissv. Hungary, §§ 73-77.

<sup>36</sup> See also the heightened requirements for technical and organizational measures when processing special categories of data, Article 29 para. 1 LED.

<sup>37</sup> CJEU - C-594/12, para. 66.

<sup>38</sup> CJEU - C-594/12, para. 67.

<sup>39</sup> CJEU - C-594/12, para. 60 and 61.

<sup>40</sup> CJEU - C-594/12, para. 68.

<sup>41</sup> CJEU - C-594/12, para. 63.

<sup>42</sup> CJEU - C-594/12, para. 64.

surveillance<sup>43</sup>. This may lead to chilling effects in regard of some or all of the fundamental rights concerned.

60. In order to facilitate and operationalise the assessment of necessity and proportionality in legislative measures related to facial recognition in the law enforcement area, the national and Union legislators could take advantage of the available practical tools especially designed for this task. In particular, the necessity and proportionality toolkit<sup>44</sup> provided by the European Data Protection Supervisor could be used.

#### *3.1.3.5 Articles 52(3), 53 of the Charter (level of protection, also in relation to that of the ECHR)*

61. According to Article 52(3) and Article 53 of the Charter, the meaning and scope of those rights of the Charter that correspond to the rights guaranteed in the ECHR must be the same as those laid down by the ECHR. While in particular for Article 7 of the Charter an equivalent may be found in the ECHR, this is not the case for Article 8 of the Charter<sup>45</sup>. Article 52(3) of the Charter does not prevent Union law to provide more extensive protection. As the ECHR does not constitute a legal instrument which has been formally incorporated into EU law, EU legislation must be undertaken in the light of the fundamental rights of the Charter<sup>46</sup>.
62. According to Article 8 of the ECHR, there shall be no interference by a public authority with the exercise of this right to respect for private and family life except when in accordance with the law and what is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.
63. The ECHR also sets standards with regard to the way limitations can be undertaken. One basic requirement, besides the rule of law, is foreseeability. In order to fulfil the requirement of foreseeability, the law must be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which and the conditions on which the authorities are empowered to resort to any such measures<sup>47</sup>. This requirement is acknowledged by the CJEU and EU data protection law (cf. section 3.2.1.1).
64. Further specifying the rights of Article 8 ECHR, the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data<sup>48</sup> have to be fully respected too. Still, it has to be considered that these provisions represent only a minimum standard in view of the prevailing Union law.

## **3.2 Specific legal framework – the Law Enforcement Directive**

---

<sup>43</sup> CJEU - C-594/12, para. 37.

<sup>44</sup> European Data Protection Supervisor: Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A toolkit (11.4.2017); European Data Protection Supervisor: EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data (19.12.2019).

<sup>45</sup> CJEU - C-203/15 - Tele2 Sverige, para 129.

<sup>46</sup> CJEU – C-311/18, para. 99.

<sup>47</sup> European Court of Human Rights, Judgment, CASE OF COPLAND v. THE UNITED KINGDOM, 03/04/2007, Application no. 62617/00, para 46.

<sup>48</sup> ETS No. 108.

65. A certain framework regarding the use of FRT is provided for in the LED. First of all, Article 3(13) LED defines the term “biometric data”<sup>49</sup>. For details, cf. section 2.1 above. Secondly, Article 8(2) clarifies that in order for any processing to be lawful it must – besides being necessary for the purposes stated in Article 1(1) LED – be regulated in national law that specifies at least the objectives of the processing, the personal data to be processed and the purpose of the processing. Further provisions of special relevance with regard to biometric data are Articles 10 and 11 LED. Article 10 has to be read in connection with Article 8 LED<sup>50</sup>. The principles for processing personal data as laid down in Article 4 LED should always be adhered to and any assessment of possible biometric processing via FRT should be guided by these.

### **3.2.1 Processing of special categories of data for law enforcement purposes**

66. According to Article 10 LED, processing of special categories of data, such as biometric data, shall be allowed only where strictly necessary and subject to appropriate safeguards for the rights and freedoms of the data subject. In addition thereto, it shall only be allowed, where authorised by Union or Member State law, to protect the vital interests of the data subject or of another natural person, or where such processing relates to data which is manifestly made public by the data subject. This general clause highlights the sensitivity of the processing of special categories of data.

#### *3.2.1.1 Authorised by Union or Member State Law*

67. Regarding the necessary type of legislative measure, recital 33 LED states that “[w]here this Directive refers to Member State law, a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned.”<sup>51</sup>.
68. According to Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms recognised by the Charter shall be ‘provided for by law’. This echoes the expression ‘in accordance with the law’ in Article 8(2) of the ECHR, which means not only compliance with applicable law, but also relates to the quality of that law without prejudice to the nature of the act, requiring it to be compatible with the rule of law.
69. Recital 33 LED states further that “[h]owever, such a Member State law, legal basis or legislative measure should be clear and precise and its application foreseeable for those subject to it, as required by the case-law of the Court of Justice and the European Court of Human Rights. Member State law regulating the processing of personal data within the scope of this Directive should specify at least the objectives, the personal data to be processed, the purposes of the processing and procedures for preserving the integrity and confidentiality of personal data and procedures for its destruction”.
70. The national law must be sufficiently clear in its terms to give data subjects an adequate indication of the circumstances in and conditions under which controllers are empowered to resort to any such measures. This includes possible preconditions for processing like specific types of evidence as well as the necessity of judicial or internal authorisation. The respective law may be technology neutral as far as the specific risks and characteristics of the processing of personal data by FRT systems are sufficiently addressed. In line with the LED and the case law of the Court of Justice of the European

---

<sup>49</sup> Art. 3(13) LED : ‘Biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

<sup>50</sup> WP258, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), p. 7.

<sup>51</sup> The type of legislative measures considered has to be in line with EU law or with the national law. Depending on the degree of interference of the restriction, a particular legislative measure, taking into account the level of norm, could be required at national level.

Union (CJEU) and of the European Court of Human Rights (ECtHR), it is indeed essential that legislative measures, which aim to provide a legal basis for a facial recognition measure, are foreseeable for the data subjects.

71. A legislative measure cannot be invoked as a law authorising the processing of biometric data by means of FRT for law enforcement purposes if it is a mere transposition of the general clause in Article 10 LED.
72. Apart from biometric data, Article 10 LED regulates the processing of other special categories of data such as sexual orientation, political opinions and religious beliefs, thus covering a broad range of processing. In addition, such a provision would lack specific requirements indicating the circumstances in and conditions under which law enforcement authorities would be empowered to resort to using facial recognition technology. Due to the reference to other types of data and the explicit need for special safeguards without further specifications, the national provision transposing Article 10 LED into national law - with a similarly general and abstract wording - cannot be invoked as a legal basis for the processing of biometric data involving facial recognition, as it would lack precision and foreseeability. In line with Articles 28(2) or 46(1)(c) LED, before the legislator creates a new legal basis for any form of processing of biometric data using facial recognition, the national data protection supervisory authority should be consulted.

### *3.2.1.2 Strictly Necessary*

73. Processing can only be regarded as "strictly necessary" if the interference to the protection of personal data and its restrictions is limited to what is absolutely necessary<sup>52</sup>. The addition of the term "strictly" means that the legislator intended the processing of special categories of data to only take place under conditions even stricter than the conditions for necessity (see above, item 3.1.3.4). This requirement should be interpreted as being indispensable. It restricts the margin of appreciation permitted to the law enforcement authority in the necessity test to an absolute minimum. In accordance with the settled case-law of the CJEU, the condition of "strict necessity" is also closely linked to the requirement of objective criteria in order to define the circumstances and conditions under which processing can be undertaken, thus excluding any processing of a general or systematic nature<sup>53</sup>.

### *3.2.1.3 Manifestly Made Public*

74. When assessing whether processing relates to data which are manifestly made public by a data subject, it should be recalled that a photograph as such is not systematically considered to be biometric data<sup>54</sup>. Therefore, the fact that a photograph has been manifestly made public by the data subject does not entail that the related biometric data, which can be retrieved from the photograph by specific technical means, is considered as having been manifestly made public.
75. As for personal data in general, for biometric data to be seen as manifestly made public by the data subject, the data subject must have deliberately made the biometric template (and not simply a facial image) freely accessible and public through an open source. If a third party discloses the biometric data, it cannot be considered that the data has been manifestly made public by the data subject.

---

<sup>52</sup> Consistent case law on the fundamental right to respect for private life, see CJEU Case C-73/07 para. 56 (Satakunnan Markkinapörssi and Satamedia); CJEU, Cases C-92/09 and C-93/09 para. 77 (Schecke and Eifert); CJEU - C-594/12, para. 52 (Digital Rights); CJEU Case C-362/14 para. 92 (Schrems).

<sup>53</sup> CJEU Case C-623/17, para 78.

<sup>54</sup> Cf. recital 51 of the GDPR: « the processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. »

76. Moreover, it is not sufficient to interpret the behaviour of a data subject to consider that biometric data has been manifestly made public. For example, in the case of social networks or online platforms, the EDPB considers that the fact that the data subject did not trigger or set specific privacy features is not sufficient to consider that this data subject has manifestly made public its personal data and that this data (e.g. photographs) can be processed into biometric templates and used for identification purposes without the data subject's consent. More generally, default settings of a service, e.g. making templates publicly available, or absence of choice, e.g. the templates are made public without the user to be able to change this setting, should not in any way be construed as data manifestly made public.

### 3.2.2 Automated individual decision-making, including profiling

77. Article 11(1) LED provides for the duty of the Member States to generally prohibit decisions based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her. As an exemption to this general prohibition, such processing may be possible only if authorised by Union or Member State law to which the controller is subject to and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller. It may only be used restrictively. This threshold applies for ordinary (i.e. not special) categories of personal data. An even higher threshold and more restrictive usage applies for the exemption under Article 11(2) LED. It re-emphasises that decisions under the first paragraph shall not be based on special categories of data, i.e. in particular biometric data for the purpose of uniquely identifying a natural person. An exemption may only be foreseen if suitable measures to safeguard the data subject's rights and freedoms and legitimate interests of the natural person concerned are in place. This exemption must be read in addition to and in the light of the premises of Article 10 LED.
78. Depending on the FRT system, even human intervention assessing the results of FRT may not necessarily provide for a sufficient guarantee by itself in respecting individuals' rights and in particular the right to the protection of personal data, considering the possible bias and error that can result from the processing itself. Furthermore, human intervention may only be considered as a safeguard if the person intervening may critically challenge the results of FRT during human intervention. It is crucial to enable the person to understand the FRT system and its limits as well as to interpret its results properly. It is also necessary to establish a work place and organisation that counteracts the effects of automation bias, and avoids fostering the uncritical acceptance of the results e.g. by time pressure, burdensome procedures, potential detrimental career effects etc.
79. According to Article 11(3) LED, profiling that results in discrimination against natural persons on the basis of special categories of personal data such as biometric data shall be prohibited, in accordance with Union law. According to Article 3(4) LED, 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. When considering whether suitable measures to safeguard the data subject's rights and freedoms and legitimate interests of the natural person concerned are foreseen, it has to be kept in mind that the use of FRT may lead to profiling, depending on the way and purpose that the FRT is applied for. In any case, in accordance with Union law and Article 11(3) LED, profiling that results in discrimination against natural persons on the basis of special categories of personal data shall be prohibited.

### 3.2.3 Categories of the data subjects

80. Article 6 LED regards the necessity to distinguish between different categories of data subjects. This distinction has to be made where applicable and as far as possible. It has to show effect in the way the data are processed. From the examples given in Article 6 LED it can be inferred that, as a rule, the processing of personal data has to meet the criteria of necessity and proportionality also with regard to the category of data subjects<sup>55</sup>. It can further be inferred that with regard to data subjects for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with the legitimate aim according to the LED, there is most likely no justification of an interference<sup>56</sup>. If no distinction according to Article 6 LED is applicable or possible, the exception from the rule of Article 6 LED has to be rigorously considered in the assessment of the necessity and proportionality of the interference. The distinction between different categories of data subjects appears as an essential requirement when it comes to personal data processing involving facial recognition, also considering the possible false positive or false negative hits, which can have significant impacts for data subjects as well as in the course of an investigation.
81. As said, when implementing Union law, the provisions of the Charter of Fundamental Rights of the European Union have to be respected, cf. Article 52 of the Charter. The framework and criteria that the LED provides are therefore to be read in the light of the Charter. Acts of law of the EU and its Member States must not fall below this measure and have to ensure the Charter's full effect.

### 3.2.4 Rights of the data subject

82. The EDPB has already provided guidance on data subjects' rights under the GDPR in different aspects<sup>57</sup>. The LED provides for similar data subject rights and general guidance on this has been provided in an opinion by Article 29 WP, which has been endorsed by the EDPB<sup>58</sup>. Under certain circumstances, the LED allows for some limitations to these rights. The parameters for such limitations will be further elaborated in section 3.2.4.6. "Legitimate limitations to data subject's rights".
83. While all data subject's rights as listed in Chapter III of the LED, naturally apply also to personal data processing via facial recognition technology (FRT), the following chapter will focus on some of the rights and aspects that might be of particular interest to receive guidance on. Furthermore, this chapter and its analysis is incumbent on the FRT processing in question having passed through the legal requirements as described in the previous chapter.
84. Given the nature of personal data processing through FRT (processing of special categories of personal data often without any apparent interaction with the data subject) the controller must carefully consider how to (or if it can) meet the requirements of the LED before any FRT processing is launched. In particular by carefully analysing:
- who the data subjects are (often more than the one(s) that is the main target for the purpose of processing),
  - how the data subjects are made aware of the FRT processing (see section 3.2.4.1),

---

<sup>55</sup> Cf. also CJEU - C-594/12, para. 56–59.

<sup>56</sup> Cf. also CJEU - C-594/12, para. 58.

<sup>57</sup> See for example 1/2022 EDPB Guidelines on data subject's rights – Right of access and 3/2019 EDPB Guidelines on processing of personal data through video devices.

<sup>58</sup> WP258, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680).

- how the data subjects can exercise their rights (here both information and access rights as well as rights to rectification or restriction can be particularly challenging to uphold in case FRT is used for all but 1-to-1 verification in direct contact with the data subject).

*3.2.4.1 Making rights and information known to data subjects in a concise, intelligible and easily accessible form*

85. FRT provides for challenges in ensuring that data subjects are made aware of their biometric data being processed. It is particularly challenging if a LEA is analysing through FRT video material that derives from or is provided by a third party since there is little possibility, and most of the time none, for the LEA to notify the data subject at the time of collection (e.g. via a sign on-site). Any video material not relevant to the investigation (or purpose for processing) should always be removed or anonymised (e.g. by blurring with no retroactive ability to recover the data) before deploying any processing of biometric data, in order to avoid the risk of not having fulfilled the minimisation principle in Article 4(1)(e) LED and the information obligations in Article 13(2) LED. It is the responsibility of the controller to assess what information would be of importance for the data subject in exercising his or her rights and to ensure that the necessary information is provided. The effective exercise of data subject's rights is dependent on the controller fulfilling its information obligations.
86. Article 13(1) LED stipulates what minimum information needs to be provided to the data subject in general. This information may be provided for via the controller's website, in printed form (e.g. a leaflet available on demand), or otherwise easy-to-access sources for the data subject. The data controller must in any event ensure that information is effectively provided in relation to at least the following elements:
  - identity and contact details of the controller, including the Data Protection Officer,
  - the purpose of the processing and that it is processing via FRT,
  - the right to lodge a complaint with a supervisory authority and contact details of such authority,
  - the right to request access to, and rectification or erasure of, personal data and restriction of processing of the personal data.
87. In addition, in specific cases as defined in national law which should be in line with Article 13(2) LED<sup>59</sup>, as for example FRT processing, the following information needs to be provided directly to the data subject:
  - the legal basis for the processing,
  - information on where the personal data was collected without the data subject's knowledge,
  - the period for which the personal data will be stored, or where that is not possible, the criteria used to determine that period,
  - if applicable, the categories of recipients of the personal data (including third countries or international organisations).
88. While Article 13(1) LED is about general information made available to the public, Article 13(2) LED is about the additional information to be provided to a particular data subject in specific cases, for example where data is collected directly from the data subject or indirectly without the knowledge of

---

<sup>59</sup> E.g. Section 56 (1) of the German Federal Data Protection Act which, amongst other, states what information needs to be provided to data subjects in undercover operations

the data subject<sup>60</sup>. There is no clear definition of what is meant with “specific cases” in Article 13(2) LED. However, it refers to situations where the data subjects need to be made aware of the processing that refers to them specifically and be provided with appropriate information in order to effectively exercise their rights. The EDPB considers that when assessing whether a “specific case” exists, several factors need to be taken into consideration, including if personal data is collected without the knowledge of the data subject, as this would be the only way to enable data subjects to effectively exercise their rights. Other examples of “specific cases” could be where personal data is further processed as subject to an international criminal cooperation procedure or in the situation of personal data being processed under covert operations as specified in national law. Furthermore, it follows from recital 38 LED that should decision-making be done solely based on FRT, then the data subjects need to be informed about the features of the automated decision making. This would also indicate that this is a specific case where additional information should be provided to the data subject in accordance with Article 13(2) LED<sup>61</sup>.

89. Finally, it should be noted that according to Article 13(3) LED, Member States may adopt legislative measures that restrict the obligation to provide information in specific cases for certain objectives. This applies to the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the data subject.

#### *3.2.4.2 Right to access*

90. In general, the data subject has the right to receive positive or negative confirmation of any processing of his or her personal data and, where the answer is positive, the access to the personal data as such, plus additional information, as listed in Article 14 LED. For FRT, when biometric data is stored and connected to an identity also by alpha-numerical data, this should allow for the competent authority to give confirmation to an access request based on a search by those alpha-numerical data and without launching any further processing of biometric data of others (i.e. by searching with FRT in a database). The principle of data minimisation must be observed and no more data than is necessary with regard to the purpose of the processing should be stored.

#### *3.2.4.3 Right to rectification of personal data*

91. Since FRT does not provide for absolute accuracy, it is of particular importance that controllers are vigilant to requests for rectification of personal data. It may also be the case when a data subject based on FRT has been placed in an inaccurate category, e.g. wrongfully put in the category of suspects based on initial assumption of course of action in a video footage. The risks for the data subjects are particularly serious if such inaccurate data is stored in a police database and/or shared with other entities. The controller must correct stored data and FRT systems accordingly, see recital 47 LED.

#### *3.2.4.4 Right to erasure*

92. FRT will under most circumstances – in case not used for 1-to-1 verification/authentication – amount to the processing of a large number of data subjects’ biometric data. It is therefore important that the controller beforehand considers where the limits to its purpose and necessity lies, so that a request for erasure in accordance with Article 16 LED can be dealt with without undue delay (since the controller needs, among others, to erase personal data that is processed beyond what the applicable legislation following Articles 4, 8 and 10 LED allows for).

---

<sup>60</sup> WP258 Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), p.17-18

<sup>61</sup> Note well the difference between “made available to the data subject” in Article 13(1) LED and “give to the data subject” in Article 13(2) LED. In Article 13(2) LED the controller must ensure that the information reaches the data subject, where published information on a website will not be sufficient.

#### *3.2.4.5 Right to restriction*

93. In case the accuracy of the data is contested by the data subject and the accuracy of the data cannot be ascertained (or when the personal data must be maintained for the purpose of future evidence), the controller has an obligation to restrict personal data of that data subject in accordance with Article 16 LED. This becomes especially important when it comes to facial recognition technology (based on algorithm(s) and thereby never showing a definitive result) in situations where large quantities of data are gathered and the accuracy and quality of the identification may vary. With poor quality video material (e.g. from a crime scene) the risk of false positives increases. Furthermore, if facial images in a watch list are not regularly updated that will also increase the risk of false positives or false negatives. In specific cases, where data cannot be erased due to the fact that there are reasonable grounds to believe that erasure could affect the legitimate interests of the data subject, the data should instead be restricted and processed only for the purpose which prevented their erasure (see recital 47 LED).

#### *3.2.4.6 Legitimate limitations to data subject's rights*

94. When it comes to the information obligations of the controller and the data subjects' right of access, limitations are allowed only so long as they are laid down in the law which in turn needs to constitute a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned (see Articles 13(3), 13(4) 15 and 16(4) LED). When FRT is used for law enforcement purposes one can expect it to be used under circumstances where it would be harmful for the purpose pursued to inform the data subject or to allow access to the data. This would apply for instance to a police investigation of a crime or in order to protect national security or public security.
95. The right of access does not automatically mean access to all the information e.g. in a criminal case where one's personal data occurs. A viable example of when limitations to the right may be allowed could be during the course of a criminal investigation.

#### *3.2.4.7 Exercise of rights through the supervisory authority*

96. In cases where there are legitimate limitations to the exercise of rights according to Chapter III LED, the data subject may request the data protection authority to exercise his or her rights on their behalf by checking the lawfulness of the controller's processing. It falls on the controller to inform the data subject of the possibility of exercising their rights in such way ( see Article 17 LED and Article 46(1)(g) LED). For FRT it means that the controller has to ensure that appropriate measures are in place so that such a request can be handled, e.g. enabling the search of recorded material provided that the data subject provides sufficient information in order to locate the personal data of him or her.

### **3.2.5 Other legal requirements and safeguards**

#### *3.2.5.1 Article 27 Data protection impact assessment*

97. A data protection impact assessment (DPIA) before the use of FRT is a mandatory requirement since the type of processing, in particular, using new technologies, and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons. Given that the use of FRT entails systematic automatic processing of special categories of data, it could be assumed that in such cases the controller would be, as a rule, required to conduct a DPIA. The DPIA should contain as a minimum a general description of the envisaged processing operations, an assessment of the necessity and proportionality of the processing operations in relation to the purposes, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address those risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance. The EDPB recommends making public the

results of such assessments, or at least the main findings and conclusions of the DPIA, as a trust and transparency enhancing measure<sup>62</sup>.

### *3.2.5.2 Article 28 Prior consultation of the supervisory authority*

98. Pursuant to Article 28 LED, the controller or processor has to consult the supervisory authority prior to the processing, where: (a) a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk; or (b) the type of processing, in particular, where using new technologies, mechanisms or procedures, involves a high risk to the rights and freedoms of data subjects. As already explained in section 2.3. of these guidelines, the EDPB considers that most cases of deployment and use of FRT contain intrinsic high risk to the rights and freedoms of data subjects. Therefore, in addition to the DPIA, the authority deploying the FRT should consult the competent supervisory authority, prior to the deployment of the system.

### *3.2.5.3 Article 29 Security of processing*

99. The unique nature of biometric data makes it impossible for a data subject to change it, in case it is compromised, e.g. as a result of a data breach. Therefore, the competent authority, implementing and/or using FRT should pay special attention to the security of processing, in line with Article 29 LED. In particular, the law enforcement authority should ensure the system complies with the relevant standards and implement biometric template protection measures<sup>63</sup>. This obligation is even more relevant if the law enforcement authority is using a third-party service provider (data processor).

### *3.2.5.4 Article 20 Data protection by design and by default*

100. Data protection by design and by default, in accordance with Article 20 LED, is aimed at ensuring that the data protection principles and safeguards, such as data minimisation and storage limitation, are embedded in the technology through appropriate technical and organisational measures, such as pseudonymisation, even before the start of the processing of personal data and will be applied throughout its lifecycle. Given the inherent high risk for the rights and freedoms of natural persons, the choice of such measures should not depend solely on economic considerations<sup>64</sup> but should instead strive to implement the state-of-art in data protection technologies. In the same vein, if a LEA intends to apply and use FRT from external providers, it has to ensure, for instance through the procurement procedure, that only FRT built upon the principles of data protection by design and by default are deployed<sup>65</sup>. This also implies that transparency on the functioning of FRT is not limited by claims of trade secrets or intellectual property rights.

### *3.2.5.5 Article 25 Logging*

101. The LED stipulates different methods of demonstrating by the controller or the processor the lawfulness of the processing and ensuring data integrity and data security. In this regard, system logs are a very useful tool and an important safeguard for verification of the lawfulness of the processing, both internally (i.e. self-monitoring) and by external supervisory authorities, such as the data protection authorities. Pursuant to Article 25 LED, logs for at least the following processing operations should be kept in automated processing systems: collection, alteration, consultation, disclosure including transfers, combination and erasure. Moreover, the logs of consultation and disclosure

---

<sup>62</sup> For more information see WP248 rev.01 Data protection impact assessment Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk".

<sup>63</sup> See for example: ISO/IEC 24745 Information security, cybersecurity and privacy protection — Biometric information protection.

<sup>64</sup> See recital 53 of the LED.

<sup>65</sup> For more information see EDPB Guidelines on Data Protection by Design and by Default, [https://edpb.europa.eu/sites/default/files/files/file1/edpb\\_guidelines\\_201904\\_dataprotection\\_by\\_design\\_and\\_by\\_default\\_v2.0\\_en.pdf](https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf).

should make it possible to establish the justification, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data. Furthermore, in the context of facial recognition systems, logging of the following additional processing operations is recommended (partly beyond Article 25 LED):

- Changes of the reference database (addition, deletion or update). The log should keep a copy of the relevant (added, deleted or updated) image, when it is not otherwise possible to verify the lawfulness or the outcome of the processing operations.
- Identification or verification attempts including the outcome and confidence score. Strict minimisation principle should apply, so that only the identifier of the image from the reference database is kept in the logs, instead of storing the reference image. Logging the input biometric data should be avoided unless there is necessity (e.g. only in match cases)
- The ID of the user who requested the identification or verification attempt.
- Any personal data stored in the logs of the systems are subject to strict purpose limitations (e.g. audits) and should not be used for other purposes (e.g. to be able to still perform recognition/verification including an image that has been deleted from the reference databases). Security measures should be applied to ensure the integrity of the logs, whereas automatic monitoring systems to detect abuse of logs are highly recommended. For the reference database logs, security measures should be equivalent to the reference database, in case of facial images storage. Also, automatic processes to ensure the enforcement of the data retention period for the logs should be implemented.

#### *3.2.5.6 Article 4(4) Accountability*

102. The controller has to be able to demonstrate the compliance of the processing with the principles of Article 4 (1)-(3), cf. Article 4(4) LED. A systematic and up-to-date documentation of the system (including updates, upgrades and algorithmic training), the technical and organisational measures (including system performance monitoring and potential human intervention) and the processing of the personal data is crucial in this regard. To demonstrate the lawfulness of the processing, a particularly important element is logging according to Article 25 LED (cf. section 3.2.5.5). The accountability principle not only refers to the system and the processing, but also to the documentation of procedural safeguards such as necessity and proportionality assessments, DPIAs as well as internal consultations (e.g. management approval of the project or internal decisions on confidence score values) and external consultations (e.g. DPA). Annex II includes a number of elements in this regard.

#### *3.2.5.7 Article 47 Effective supervision*

103. The effective supervision by the competent data protection authorities is one of the most important safeguards for the fundamental rights and freedoms of the individuals affected by the use of FRT. At the same time, providing each data protection authority with the necessary human, technical and financial resources, premises and infrastructure is a prerequisite for the effective performance of their tasks and exercise of their powers<sup>66</sup>. Even more crucial than the number of available staff, are the skills of the experts, who should cover a very broad range of issues - from criminal investigations and police cooperation to big data analytics and AI. Therefore, Member States should ensure that the resources

---

<sup>66</sup> See Commission Communication “First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 (‘LED’), COM(2022) 364 final, p. 3.4.1.

of the supervisory authorities are appropriate and sufficient to allow them to fulfil their mandate to protect the rights of data subjects and closely follow any developments in this regard.<sup>67</sup>

## 4 CONCLUSION

104. The use of facial recognition technologies is intrinsically linked to processing of significant amounts of personal data, including special categories of data. The face and, more generally, biometric data are permanently and irrevocably linked to a person's identity. Therefore, the use of facial recognition has direct or indirect impact on a number of fundamental rights and freedoms enshrined in the EU Charter of Fundamental Rights that may go beyond privacy and data protection, such as human dignity, freedom of movement, freedom of assembly, and others. This is particularly relevant in the area of law enforcement and criminal justice.
105. The EDPB understands the need for law enforcement authorities to benefit from the best possible tools to quickly identify the perpetrators of terrorist acts and other serious crimes. However, such tools should be used in strict compliance with the applicable legal framework and only in cases when they satisfy the requirements of necessity and proportionality, as laid down in Article 52(1) of the Charter. Moreover, while modern technologies may be part of the solution, they are by no means a 'silver bullet'.
106. There are certain use cases of facial recognition technologies, which pose unacceptably high risks to individuals and society ('red lines'). For these reasons the EDPB and the EDPS have called for their general ban<sup>68</sup>.
107. In particular, remote biometric identification of individuals in publicly accessible spaces poses a high risk of intrusion into individuals' private lives and does not have a place in a democratic society, as by its nature, it entails mass surveillance. In the same vein, the EDPB considers AI-supported facial recognition systems categorising individuals based on their biometrics into clusters according to ethnicity, gender, as well as political or sexual orientation as not compatible with the Charter. Furthermore, the EDPB is convinced that the use of facial recognition or similar technologies, to infer emotions of a natural person is highly undesirable and should be prohibited, possibly with few duly justified exceptions. In addition, the EDPB considers that processing of personal data in a law enforcement context that would rely on a database populated by collection of personal data on a mass-scale and in an indiscriminate way, e.g. by "scraping" photographs and facial pictures accessible online, in particular those made available via social networks, would, as such, not meet the strict necessity requirement provided for by Union law.

## 5 ANNEXES

Annex I: Support Pattern

Annex II: Practical guidance for managing FRT projects in LEAs

---

<sup>67</sup> See Contribution of the EDPB to the European Commission's evaluation of the Data Protection Law Enforcement Directive (LED) under Article 62, para. 14, [https://edpb.europa.eu/system/files/2021-12/edpb\\_contribution\\_led\\_review\\_en.pdf](https://edpb.europa.eu/system/files/2021-12/edpb_contribution_led_review_en.pdf)

<sup>68</sup> See 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) [https://edpb.europa.eu/system/files/2021-06/edpb-edps\\_joint\\_opinion\\_ai\\_regulation\\_en.pdf](https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf)

### Annex III: Practical Examples

## ANNEX I - TEMPLATE FOR DESCRIPTION OF SCENARIOS

**(With infoboxes for aspects dealt within the scenario)**

### **Description of the processing:**

- Description of the processing, Context (crime relation), Purpose

### **Source of information:**

- Types of data subjects:  all citizens       convicts       suspects  
 children       other vulnerable data subjects
- Source of image:  publicly accessible spaces       internet  
 private entity       other individuals       other .....
- Connection to crime:  Direct temporal       Not direct temporal  
 Direct geographical       Not direct geographical  
 Not necessary
- Mode of information capture:  remote       in a booth or controlled environment
- Context- affecting other fundamental rights:
  - No
  - Yes, namely       freedom of assembly  
 Freedom of speech  
 various:.....
- Possibilities for additional sources of information about the data subject:
  - ID document       public telephone use       vehicle license plate
  - other .....

### **Reference database (to which captured information is compared):**

- Specificity:  general purpose databases       specific databases related to crime area
- Description of how these reference databases were populated (and legal basis)
- Change of purpose of database (e.g. security of private property was the primary goal): YES  
 NO

### **Algorithm:**

- Processing type:  1-1 verification (authentication)       1-many identification
- Accuracy considerations
- Technical safeguards

### **Outcome:**

- Impact  Direct (e.g. the data subject may be arrested, questioned, discriminatory behavior)  
 Not direct (used for statistical models, no serious legal action against data subjects)
- Automated decision:  YES       NO
- Duration of storage

### **Legal analysis:**

- Necessity and proportionality analysis - purpose/seriousness of crime/number of persons not involved but affected by processing
- Type of prior information to data subject:  When entering the specific area  
 In the LEA's website in general  
 In the LEA's website for the specific processing  
 Other .....
- Applicable legal framework:
  - LED mostly copied to national law
  - Generic national law for the use of biometric data by LEAs
  - Specific national law for this processing (facial recognition) for that competent authority
  - Specific national law for this processing (automated decision)

### **Conclusion:**

General considerations as to whether the described processing is likely compatible with EU Law (and some hints to legal prerequisites)

## ANNEX II- PRACTICAL GUIDANCE FOR MANAGING FRT PROJECTS IN LEAS

This Annex provides some additional practical guidance for Law Enforcement Authorities ("LEAs") planning to initiate a project involving Facial Recognition Technology ("FRT"). It provides more information on organizational and technical measures to consider during the deployment of the project and should not be considered as an exhaustive list of steps/measures to take. It should also be seen in conjunction with the EDPB [Guidelines 3/2019 on processing of personal data through video devices<sup>69</sup>](#) and any EU/EEA regulation and EDPB guidelines regarding the use of Artificial Intelligence.

This Annex provides guidelines based on the assumption that LEAs will procure FRT (as off-the-shelf products). If the LEA plans to develop (further train) the FRT, then additional requirements apply for selecting the necessary training, validation and testing datasets to be used during development and the roles/measures for the development environment. Similarly, an off-the-shelf product may require further adjustments for the intended use, in which case above mentioned requirements for the selection of testing, validation and training datasets should be met.

Belonging to the same LEA does not provide on its own full access to biometric data. As with any other personal data categories, biometric data collected for a certain law enforcement purpose under a specific legal basis cannot be used without a proper legal basis for a different law enforcement purpose (Article 4(2) of Directive (EU) 2016/680 (LED)). Also, developing/training an FRT tool is considered a different purpose and it should be assessed whether processing biometric data to measure performance/train the technology so to avoid impact on the data subjects by low performance is necessary and proportionate taking into account the initial purpose of processing.

### 1. ROLES AND RESPONSIBILITIES

When a LEA employs FRTs for the performance of its tasks falling under the scope of the LED (prevention, investigation detection or prosecution of criminal offences, etc., according to Article 3 LED), it can be considered the controller for the FRT. However, LEAs are composed of several units/departments that may be involved in this processing, either by defining the process of FRT application, or by applying it in practice. Due to the specificities of this technology, different units may need to be involved to either support in the measurements of its performance, or to further train it.

In a project involving FRT, there are several stakeholders<sup>70</sup> within LEAs that may need to be involved:

- Top management - to approve the project after balancing the risks against the potential benefits.
- DPO and/or legal department of the LEA - to assist in assessing the lawfulness of implementing a certain FRT project; to assist in carrying out the DPIA; to ensure the respect and exercise of the rights of the data subjects.

---

<sup>69</sup> [https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-3-2019-processing-personal-data-through-video\\_en](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-3-2019-processing-personal-data-through-video_en).

<sup>70</sup> The following roles are indicative of the different stakeholders and their responsibilities in an FRT project. While the language used to describe the roles in this annex is not assertive, each LEA needs to define and assign similar roles according to its organisation. It might be the case that a unit accumulates more than one role, for instance process owner and reference database manager, or process owner and IT AI and/or Data Science Department (in case the unit of the process owner has all necessary technical knowledge).

- Process Owner - acting as the specific unit within the competent LEA to develop the project, deciding the details of the FRT project, including the system performance requirements; deciding on the appropriate fairness metric; setting the confidence score<sup>71</sup>; setting acceptable thresholds for bias; identifying the potential risks the FRT project poses for the rights and freedoms of the individuals (by consulting also the DPO and the IT AI and/or Data Science Department (see below) and to present them to the top management. The process owner will also consult the reference database manager, before deciding on the details of the FRT project, to understand both the use purpose of the reference database but also its technical details. In case of re-training a procured FRT, the Process Owner will also be in charge of the selection of the training dataset. As being the unit tasked with developing and deciding the details of the project, the process Owner is in charge of conducting the DPIA.
- IT AI and/or Data Science Department - to assist in carrying out a DPIA; to explain the metrics available to measure the system performance, fairness<sup>72</sup> and potential bias; to implement the technology and the technical safeguards, in order to prevent unauthorized access to the collected data, cyberattacks, etc. In case of re-training a procured FRT, the IT AI or Data science department will train the system, based on the training dataset provided by the Process Owner. This department will also be in charge of setting up the measures to mitigate the risks jointly identified by the process owners (e.g. AI specific risks such as model inference attacks).
- End users (such as the police officers in the field or in forensics labs) - to carry out a comparison against the database; to critically review the results taking into account previous evidence and provide feedback to the Process Owner for false positive results and indications of possible discrimination.
- Reference database manager - the specific unit within the competent LEA in charge of accumulating and managing the reference database, meaning the database against which images will be compared, including deleting facial images after the defined retention period. Such database can be created specifically for the envisaged FRT project or can pre-exist, for compatible purposes. The reference database manager is in charge of defining when and under which circumstances facial images can be stored as well as setting their data retention requirements (according to time or other criteria).

As most cases of deployment and use of FRT contain intrinsic high risk to the rights and freedoms of data subjects, the Data Protection Supervisory Authority should also be involved in the context of the prior consultation required by Article 28 LED.

## 2. INCEPTION/BEFORE PROCURING THE FRT SYSTEM

The Process Owner in a LEA should first have a clear understanding of the process(es) pursuing the use of FRT (the use case/s) and ensure there is a legal basis to ground the intended use case. Based on this, they need to:

- Describe formally the use case. The problem to be solved and the way FRT will provide a solution is to be described, as well as the overview of the process (task) in which it will be applied. In this regard, the LEAs should document at least<sup>73</sup>:

---

<sup>71</sup> Confidence score is the confidence level of the prediction (match), in the form of a probability. E.g. by comparing two templates, there is 90% confidence that these belong to the same person. Confidence score is different than the performance of the FRT, however it affects the performance. The higher the confidence threshold, the fewer false positives and more false negatives in the results of FRT.

<sup>72</sup> Fairness can be defined as the lack of unfair, unlawful discrimination, such as gender or race bias.

<sup>73</sup> Annex I provides a list of elements assisting the controller to describe an FRT use case.

- The categories of personal data recorded in the process
- The objectives and concrete purposes for which the FRT will be used, including the potential consequences for the data subject after a match.
- When and how the facial images will be collected (including information on the context of this collection, e.g. at the airport gate, videos from security cameras outside a store where a crime was committed etc. and the categories of data subjects whose biometric data will be processed).
- The database against which images will be compared (reference database), as well as information on how it was created, its size and the quality of biometric data it contains.
- The LEA actors who will be authorized to use the FRT system and act upon it in the law enforcement context (their profiles and access rights have to be defined by the Process Owner).
- The envisaged retention period for the input data, or the moment that will determine the end of this period (such as the closure or termination of the criminal proceedings in accordance with national procedural law for which they have been initially collected), as well as any subsequent action (deletion of this data, anonymisation and use for statistical or research purposes etc.).
- Logging implementation and accessibility of logs and records kept.
- The performance metrics (e.g. accuracy, precision, recall, F1-score) and their minimum acceptable thresholds.<sup>74</sup>
- An estimation of how many people will be subject to FRT in which time period / occasion.
- Perform a necessity and proportionality assessment<sup>75</sup>. The fact that this technology exists should not be the driver to apply it. The Process Owner must first assess whether an appropriate legal basis for the envisaged processing exists. For this, the DPO and the legal service need to be consulted. The driver to deploy FRT should be that it is necessary and proportionate solution for a specifically defined problem of LEAs. This needs to be assessed according to the purpose/seriousness of crime/number of persons not involved but affected by the FRT system. For the assessment of lawfulness, at least the following should be considered: LED<sup>76</sup>, GDPR<sup>77 78</sup> any existing legal framework on AI<sup>79</sup> and all accompanying guidelines provided by data protection supervisory authorities (such as the EDPB guidelines 3/2019 on processing of personal data

<sup>74</sup> There are different metrics to evaluate the performance of an FRT system. Each metric provides a different view of the system results and its success in providing an adequate picture of whether the FRT system is performing well or not depends on the use case of FRT. If the focus is on achieving high percentages of correct matching a face, metrics such as precision and recall could be used. However, these metrics do not measure how well the FRT handles negative examples (how many were incorrectly matched by the system). The Process Owner, supported by the IT AI and Data Science Department should be able to set the performance requirements and express them in the most suitable metric according to the FRT use case.

<sup>75</sup> Further steps to take care of necessity may be considered as to the tailoring and use of the system, so the description of the use case may also be slightly changed during the necessity and proportionality assessment.

<sup>76</sup> 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.

<sup>77</sup> 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.

<sup>78</sup> In cases where a scientific project aiming at researching the use of FRT would need to process personal data, but such processing would not fall under Article 4 (3) LED, generally, the GDPR would be applicable (Article 9(2) LED). In case of pilot projects that would be followed by law enforcement operations, the LED would still be applicable.

<sup>79</sup> For example, there is a proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS, however this is not yet established as a regulation.

through video devices<sup>80</sup>). These acts of EU legislation should always be corroborated with the applicable national requirements, especially in the area of criminal procedural law. The proportionality assessment should identify the fundamental rights of data subjects which may be affected (beyond privacy and data protection). It should also describe and consider any limits (or lack of limits) imposed in the use case to the FRT system. For example, if the system will run continuously or temporarily and if it will be limited to a geographical area.

- Perform a Data Protection Impact Assessment (DPIA)<sup>81</sup>. A DPIA should be conducted since the deployment of FRT in the law enforcement area is prone to result in a high risk for the rights and freedoms of the individuals<sup>82</sup>. The DPIA should contain in particular: a general description of the envisaged processing operations<sup>83</sup>, an assessment of the risks to the rights and freedoms of data subjects<sup>84</sup>, the measures envisaged to address those risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance. The DPIA is an ongoing process, so any new elements of the processing should be added and the risk assessment should be updated in each stage of the project.
- Get approval from top management by explaining the risks to the rights and freedoms of data subjects (from the use case and the technology) and the respective risk treatment plans.

### 3. DURING PROCUREMENT AND BEFORE DEPLOYMENT OF THE FRT

- Decide the criteria to select the FRT (algorithm). The Process Owner should decide the criteria to select an algorithm, with the help of the IT AI and/or Data Science department. In practice, these would include fairness and performance metrics decided in the description of the use case. Such criteria should also include information relating to data the algorithm was trained with. The training, testing and validation set need to sufficiently include samples of all characteristics of data subjects to be subject to the FRT (consider for example, age, gender and race) to reduce bias. The FRT provider should provide information and metrics on the FRT training, testing and validation datasets, and describe the measures taken to measure and mitigate potential unlawful discrimination and bias. The Process Owner, where possible, has to check whether there was a legal basis for the provider to use this dataset for the purpose of the training the algorithms (based on information the provider will make available). Also, the Process Owner should ensure that the FRT provider applies biometric data related security standards, such as ISO/IEC 24745, which provides guidance for the protection of biometric information under various requirements for confidentiality, integrity and renewability/revocability during storage and transmission and

---

<sup>80</sup> [https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-3-2019-processing-personal-data-through-video\\_en](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-3-2019-processing-personal-data-through-video_en).

<sup>81</sup> Further guidance on DPIAs can be found at: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, WP 248 rev.01, available at: <https://ec.europa.eu/newsroom/article29/items/611236> and the EDPS Accountability on the ground toolkit, part II, available at: [https://edps.europa.eu/node/4582\\_en](https://edps.europa.eu/node/4582_en)

<sup>82</sup> FRT, depending on the use case may fall under the following criteria triggering high-risk processing (from Guidelines on DPIA, WP 248 rev.01): Systematic monitoring, data processed on a large scale, matching or combining datasets, innovative use or applying new technological or organizational solutions.

<sup>83</sup> The description of the processing as well as necessity and proportionality assessment as already described in the above steps are also part of the DPIA, apart from risk assessment. If need be, a more detailed description of the personal data flows will be provided in the DPIA.

<sup>84</sup> The analysis of the risks to the data subjects should include risks related to the place of the facial images to be compared (local/remote), risks related to processors/sub-processors, as well as risks specific to machine learning when this is applied (e.g. data poisoning, adversarial examples).

requirements and guidelines for the secure and privacy-compliant management and processing of biometric information.

- Retrain the algorithm (if necessary). The Process Owner should ensure that fine-tuning the FRT system for achieving higher accuracy before its use is also part of the procured services. In case additional training of the acquired FRT system is necessary to meet the accuracy metrics, the Process Owner, apart from taking the decision to retrain, needs to decide, with the help of IT AI and/or Data Science Department on the adequate, representative dataset to be used and check the lawfulness of this use for the data.
- Set the appropriate safeguards to treat risks related to security, bias and low performance. This includes establishing a process to monitor the FRT once in use (logging and feedback for the accuracy and fairness of results). In addition, ensure the risks which are specific to some machine learning and FRT systems (e.g. data poisoning, adversarial examples, model inversion, white-box inference) are identified, measured and mitigated. The Process Owner should also set appropriate safeguards to ensure data retention requirements for biometric data included in the re-training dataset will be respected.
- Document the FRT system. This should include a general description of the FRT system, a detailed description of the elements of the FRT system and of the process for its establishment, detailed information about the monitoring, functioning and control over the FRT system and a detailed description of its risks and mitigation measures. The elements included in this documentation will include main elements of the FRT system description from previous phases (see above), however these will be enhanced with information related to monitoring performance and applying changes to the system, including any version updates and/or re-training.
- Create user manuals, explaining the technology and the use cases. These need to explain all scenarios and prerequisites under which FRT will be used) in a clear manner.
- Train the end users on how to use the technology. Such trainings need to explain the capabilities and limitations of the technology so that the users can understand the circumstances under which it is necessary to apply it and the cases in which it can be inaccurate. Such trainings will also assist in mitigating risks relating to not checking/criticizing the algorithm outcome.
- Consult the data protection supervisory authority, pursuant to Article 28(1)(b) LED. Provide information following Article 13 LED to inform the data subjects about the processing and their rights. These notices need to address the data subjects in appropriate language so that they are able to understand the processing and explain the basic elements of the technology, including accuracy rates, training datasets and measures taken to avoid discrimination and low accuracy of the algorithm.

## 4. RECOMMENDATIONS AFTER DEPLOYMENT OF THE FRT

- Ensure human intervention and oversight of the results. Never take any measure concerning an individual solely based on the outcome of the FRT (this would imply a breach of Article 11 of the LED- automated individual decision-making having legal or other similar effects on the data subject). Ensure that a LEA officer reviews the results of the FRT. Also ensure that LEA users avoid automation bias, by investigating contradictory information and critically challenging the results of the technology. For this, continuous training and awareness raising to the end users is important, however the top management should ensure there are adequate human resources to perform effective oversight. This entails providing enough time to each agent to critically challenge the results of the technology. Record, measure and assess to which extent the human oversight changes the FRT original decision.
- Monitor and address FRT model drift (performance degradation) once the model is in production.

- Establish a process to re-assess the risks and the security measures regularly and every time the technology or use case suffers any changes.
- Document any change to the system throughout its lifecycle (e.g. upgrades, re-training).
- Establish a process as well as the related technical capabilities to address access requests by the data subjects. Technical capability for the extraction of data, should there be a need to provide them to data subjects, needs to be in place before any request comes up.
- Ensure that there are procedures in place for data breaches. Should a personal data breach occur, involving biometric data, the risks are likely to be high. In this case all involved users should be aware of the relevant procedures to follow, the DPO should immediately be informed and the data subjects be informed.

## ANNEX III - PRACTICAL EXAMPLES

There are many different practical settings and purposes of using facial recognition, such as in controlled environments like in border crossings, cross-checking with data from police databases, or from personal data manifestly made public by the data subject, live camera feeds (live facial recognition), etc. As a result, the risks for the protection of personal data and other fundamental rights and freedoms vary significantly in the different use cases. In order to facilitate the necessity and proportionality assessment, which should precede the decision on the possible deployment of facial recognition, the current guidelines provide a non-exhaustive list of possible applications of FRT in the law enforcement field.

The scenarios presented and assessed are based on **hypothetical** situations and are intended to illustrate certain concrete uses of FRT and provide assistance for case-by-case considerations, as well as setting an overall framework. They do not aspire to be exhaustive and are without prejudice to any ongoing or future proceedings undertaken by a national supervisory authority with regard to the design, experimentation or implementation of facial recognition technologies. The presentation of these scenarios should serve only the purpose of exemplifying the guidance to policy makers, legislators and law enforcement authorities, already provided in this document, when devising and envisioning the implementation of facial recognition technologies in order to ensure full compliance with the EU acquis in the field of personal data protection. In this context, it should be borne in mind that even in similar situations of using FRT, the presence, or the absence, of certain elements may lead to a different outcome of the necessity and proportionality assessment.

### 1 SCENARIO 1

#### 1.1. Description

An Automated Border Control system which allows for an automated border passage by authenticating the biometric image stored in the electronic travel document of EU citizens and other travellers passing the border passage and establishing that the passenger is the rightful holder of the document.

Such verification/authentication involves only one-to-one facial recognition and is carried out in controlled environment (e.g. at airport e-gates). The biometric data of the traveller passing the border passage are captured when he/she is explicitly prompted to look at the camera in the e-gate and is compared to that of the presented document (passport, identity card, etc.) which is issued following specific technical requirements.

At the same time, while the processing in such cases in principle falls outside the scope of the LED, the outcome of the verification may also be used in matching (alphanumeric) data of the person against law enforcement databases as part of the border control and thus may entail actions with significant legal effect for the data subject, e.g. arrest pursuant to an alert in SIS. Under specific circumstances, the biometric data can be also used to search for matches in law enforcement databases (in such a case 1-many identification would be performed in this step).

The outcome of the biometric image processing has a direct impact on the data subject: only in case of successful verification it allows passing the border passage. In case of unsuccessful identification, the border guards need to perform a second check to ensure the data subject is different than the one depicted in the identification document.

In case a SIS or national alert is identified, the border guards need to perform a second verification and the necessary further checks and then take any necessary action, e.g. arrest the person, inform concerned authorities.

Source of information:

- Types of data subjects:  all individuals crossing the borders
- Source of image:  other (ID document)
- Connection to crime:  Not necessary
- Mode of information capture:  in a booth or controlled environment
- Context - affecting other fundamental rights: Yes, namely:  right to free movement  right to asylum

Reference database (to which captured information is compared):

- Specificity:  specific databases related to border control

Algorithm:

- Verification type:  1-1 verification (authentication)

Outcome:

- Impact  Direct (the data subject is allowed or denied entry)
- Automated decision:  Yes

## 1.2. Applicable legal framework

Since 2004, pursuant to Council Regulation (EC) No 2252/2004<sup>85</sup>, passports and other travel documents issued by Member States have to contain a biometric facial image stored in an electronic chip embedded in the document.

The Schengen Borders Code (SBC)<sup>86</sup> lays down the requirements for border checks on persons at the external borders. For EU citizens and other persons enjoying the right of free movement under Union law, the minimum checks should consist of a verification of their travel documents, where appropriate by using technical devices. The SBC has been subsequently amended with Regulation (EU) 2017/2225<sup>87</sup>, which has introduced, *inter alia*, definitions for ‘e-gates’, ‘automated border control system’ and ‘self-service system’, as well as the possibility for processing biometric data for carrying out border checks.

Hence, it could be assumed that there is a clear and foreseeable legal basis authorising this form of personal data processing. Moreover, the legal framework is adopted at Union level and is directly applicable to Member States.

## 1.3. Necessity and proportionality - purpose/seriousness of crime

Verification of the identity of EU citizens in an automated border control, using their biometric image, is an element of the border checks at the external borders of the EU. Consequently, it is directly related to border security and serves an objective of general interest recognized by the Union. In addition, ABC gates help to speed up the processing of passengers and lessen the risk of human errors. Furthermore, the scope, the extent and the intensity of the interference in this scenario is much more limited compared with other forms of facial recognition. Nevertheless, the processing of biometric data

<sup>85</sup> COUNCIL REGULATION (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States.

<sup>86</sup> REGULATION (EU) 2016/399 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code).

<sup>87</sup> Regulation (EU) 2017/2225 of the European Parliament and of the Council of 30 November 2017 amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System.

creates additional risks for the data subjects which need to be properly addressed and mitigated by the competent authority deploying and operating the FRT.

#### 1.4. Conclusion

The verification of the identity of EU citizens in the context an automated border control is a necessary and proportionate measure, as long as the appropriate safeguards are in place, in particular the application of the principles of purpose limitation, data quality, transparency and a high level of security.

## 2 SCENARIO 2

### 2.1. Description

A system of identification of victims of child abduction is set by the LEAs. An authorised police officer may carry out a comparison of the biometric data of a child, suspected to be abducted, against a database of victims of child abduction under strict conditions, for the sole purpose of identifying minors who may correspond to the description of the missing child for which an investigation has been initiated and the alert issued.

The processing at stake would be the comparison of the face or image of an individual, who may correspond to the description of a missing child, with the images stored in the database. Such processing would happen in specific cases and not on a systematic basis.

The database against which the comparison will be applied is populated with pictures of missing children for which a suspicion of child abduction, a threat to the child's life or physical integrity, has been reported and a criminal investigation has been opened under a judicial authority, and for which an alert for child abduction has been issued. Data are collected within the framework of procedures established by the competent law enforcement authority, that is police officers authorized to carry out judicial police missions. The categories of personal data recorded are:

- identity, nickname, alias, filiation, nationality, addresses, e-mail addresses, telephone numbers;
- date and place of birth;
- parentage information;
- photograph with technical features allowing the use of a facial recognition device and other photographs.

Comparison results must also be reviewed and verified by an authorised officer, in order to corroborate previous evidence with the result of the comparison and rule out any possible false positive results.

Children's pictures and personal data may be retained only for the duration of the alert and must be deleted immediately after the closure or termination of the criminal proceedings in accordance with national procedures for which they have been inserted into the database.

While the retention period for biometric data in the database may be envisioned for a relatively long period of time and defined as per national law, the exercise of data subject rights and in particular the right to rectification and erasure provides for an additional guarantee to limit the interference with the right to the protection of personal data of the data subjects concerned.

Source of information:

- Types of data subjects:  Children
- Source of image  other: not predefined, suspected victim of child abduction
- Connection to crime  Not direct temporal  Not direct geographical
- Mode of information capture:  in a booth or controlled environment
- Context: affecting other fundamental rights  Yes, namely:  various

Reference database (to which captured information is compared):

- Specificity  specific database

Algorithm:

- Verification type:  1-many identification

Outcome:

- Impact  Direct
- Automated decision:  NO, mandatory review by an authorized officer

Legal analysis:

- Applicable legal framework:  Specific national law for this processing (facial recognition)

## 2.2. Applicable legal framework

National law provides for a dedicated legal framework establishing the database, determining the purposes of processing as well as the criteria for the database to be populated, accessed and used. The legislative measures necessary for its implementation also provide for the determination of a retention period as well as referring to the applicable principles of integrity and confidentiality. The legislative measures also foresee the modalities for the provision of information to the data subject and in this case the holder(s) of parental responsibility, as well as the exercise of data subject rights and possible limitation if applicable. During the preparation of the proposal for the respective legislative measure, the national supervisory authority had to be consulted.

## 2.3. Necessity and proportionality - purpose/seriousness of crime/number of persons not involved but affected by processing

Conditions and safeguards for processing

The facial recognition comparison can only be carried out by an authorised officer as a last resort unless there are no other less intrusive means available and where strictly necessary, for instance, in case there is doubt about the authenticity of a traveling minor's identity document and/or after having reviewed previous evidence and material gathered indicating a possible correspondence with the description of a missing child for which a criminal investigation is being carried out.

An additional safeguard is also provided with the mandatory review and verification of the facial recognition comparison by an authorised officer, in order to corroborate previous evidence with the result of the comparison and rule out any possible false positive results.

Objective pursued

The establishment of the database serves important objectives of general public interest, in particular the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and the protection of the rights and freedoms of others. The establishment of the database and the processing foreseen appears to contribute to the identification of children victim of

abduction and therefore can be considered as a measure suitable to support the legitimate objective to investigate and prosecute such crime.

#### Purpose and population of the database

The purposes of processing are clearly defined by law and the database shall be used only for the purpose of identifying missing children for which a suspicion of child abduction has been reported and a criminal investigation has been initiated under the supervision of a judicial authority and for which an alert for the child abduction has been issued. The conditions set out by law for the population of the database aim at strictly limiting the number of data subjects and personal data to be included in the database. The holder of parental responsibility over the child must be informed about the processing undertaken and the conditions for the exercise of the child's rights in relation to the biometric processing envisioned for the purpose of identification, or to the child personal data stored in the database.

#### 2.4. Conclusion

Considering the necessity and proportionality of the processing envisioned, as well as the best interest of the child in carrying out such personal data processing, and provided that sufficient guarantees are in place to notably ensure the exercise of data subject rights – in particular taking into account the fact that children's data are to be processed, such application of facial recognition processing may be considered as likely compatible with EU law.

Furthermore, given the type of processing and the technology used, which involves a high risk to rights and freedoms of data subject concerned, the EDPB considers that the preparation of a proposal for a legislative measure to be adopted by a national parliament or of a regulatory measure based on such a legislative measure, which relates to the envisioned processing, must include a prior consultation of the supervisory authority in order to ensure consistency and compliance with the applicable legal framework, cf. Art. 28.2 LED.

### 3 SCENARIO 3

#### 3.1. Description

In course of police interventions in riots and investigations afterwards, a number of persons have been identified as suspects, e.g. by previous investigations using CCTV coverage or witnesses. Pictures of these suspects are compared with pictures of persons who were recorded on CCTV or mobile devices at a crime scene or in surrounding areas.

In order to obtain more detailed evidence on persons suspected of having participated in riots surrounding a demonstration, the police creates a database consisting of image material with a loose local and temporal connection to the riots. The database includes private recordings uploaded to the police by citizens, material from public transport CCTV, police-owned video surveillance material and material published by the media without any specific limitation or safeguard. The display of severe criminal behaviour is not a prerequisite for the collection of the files in the database. Therefore, persons not involved in the riots – a significant percentage of the local population who happened to pass by at the moment of the demonstration, or participated in the demonstration but not in the riots – are stored in the database. It amounts to thousands of video and image files.

Using a facial recognition software, all faces appearing in those files are assigned to unique face ID's. The faces of individual suspects are then automatically compared to these face ID's. The database consisting of all biometric templates in the thousands of video and images files is stored until all

possible investigations are terminated. Positive matches are dealt with by responsible officers, who then decide on further action. This may include to attribute the file found in the database to the respective person's criminal file as well as further measures, such as questioning or arrest of that person.

A national law provides for a generic provision, according to which the processing of biometric data for the purpose of uniquely identifying a natural person is admissible if strictly necessary and subject to appropriate safeguards for the rights and freedoms of the person concerned.

Source of information:

- Types of data subjects:  all persons
- Source of image:  publicly accessible spaces  private entity  other individuals  other media
- Connection to crime:  Not necessarily direct geographical or temporal connection
- Mode of information capture:  remote
- Context - affecting other fundamental rights: Yes, namely  freedom of assembly context
- Available additional sources of information about the data subject:  
 other: not excluded (such as usage of ATM-machines or shops entered), as no control over motives on pictures may be exercised

Reference database (to which captured information is compared):

- Specificity:  specific databases related to crime area

Algorithm:

- Processing type:  1-many identification

Outcome:

- Impact:  Direct (e.g. the data subject may be arrested, questioned)
- Automated decision:  NO
- Duration of storage: until all possible investigations are terminated

Legal analysis:

- Type of prior information to data subject:  In the LEA's website in general
- Applicable legal framework :  LED mostly copied to national law  Generic national law for the use of biometric data by LEAs

### 3.2. Applicable legal framework

As clarified above, legal bases merely repeating the general clause of Article 10 LED are not sufficiently clear in their terms to give individuals an adequate indication of conditions and circumstances in which LEAs are empowered to use CCTV recordings from public spaces for creating a biometric template of their face and compare it to police databases, other available CCTV or private recordings etc. The legal framework established in this scenario therefore fails to meet the minimum requirements to serve as a legal base.

### 3.3. Necessity and proportionality

In this example, the processing raises various concerns under the necessity and proportionality principles for several reasons:

Persons are not suspected of a serious crime. The display of severe criminal behaviour is not a prerequisite for the use of the files in the database containing the image material. Also, a direct temporal and geographical connection to the crime is not a prerequisite for the use of the files in the database. This results in a significant percentage of the local population being stored in a biometric database for a duration of potentially several years, until all investigations are terminated.

The crime scene database is not limited to images fulfilling the proportionality requirements, thus leading to an unlimited amount of images to compare. This contradicts the principle of data minimisation. A smaller amount of images would also enable non-algorithmic and less intrusive means to be considered, e.g. super recognizers.<sup>88</sup>

As the example is drawn from surroundings of a protest, it is also likely that images reveal political opinions of participants in the demonstration, being the second special category of data possibly affected in this scenario. In this scenario, it is unclear how the collection of this data can be prevented and with what safeguards. Moreover, when data subjects learn that their participation in a demonstration has resulted in their entry in a biometric police database, this can have serious chilling effects on their future exercise of their right to assembly.

The biometric templates in the database can also be compared with one another. This allows the police not only to look for a specific person in all of their material but also to re-create a person's behavioural pattern over a period of several days. It can also gather additional information on the persons such as social contacts and political involvement.

The interference is further intensified by the fact that the data is processed without the knowledge of the data subjects.

Bearing in mind that photographs and videos are recorded by persons all the time, and that even the omnipresent CCTV-coverage may be analysed biometrically, this can lead to severe chilling effects.

The extensive usage of private photographs and videos, including potential misuse like denunciation, is another point of concern. As misuse like denunciation is a risk also inherent to criminal proceedings in general, the risk is considerably higher as to the scalability of the data processed and the number of the persons involved, as people might upload also material relating to a specific person or group of persons of dislike. Requests by the police to upload photographs and videos possibly lead to very low thresholds for people to provide material, especially as it might be possible to do so anonymously or at least without the need to show up and identify oneself at a police station.

### 3.4. Conclusion

In the example, there is no specific provision which could serve as a legal base. However, even if there was a sufficient legal base, the necessity and proportionality requirements would not be met, thus resulting in a disproportionate interference with the data subject's rights to respect for private life and the protection of personal data under the Charter.

---

<sup>88</sup> I.e. people with extraordinary face-recognition ability. Cf. also: Face Recognition by Metropolitan Police Super-Recognisers, 2016 Feb 26, DOI: 10.1371/journal.pone.0150036, <https://pubmed.ncbi.nlm.nih.gov/26918457/>.

## 4 SCENARIO 4

### 4.1. Description

The police implements a way of identifying suspects committing a serious crime caught on CCTV by retrospective FRT. An officer manually selects image(s) of suspects in the video material that has been collected from the crime scene or elsewhere within a preliminary investigation and then sends the image(s) to the forensic department. The forensic department uses FRT to match these image(s) to pictures of individuals that have previously been gathered in a database by the police (a so called description database that consists of suspects and former convicts). The description database is for this procedure – temporarily and in an isolated environment – analysed with FRT in order to be able to carry out the matching process. To minimize the interference with the rights and interests of the persons matched, a very limited number of employees at the forensic department have permission to conduct the actual matching procedure, access to the data is restricted to those officers entrusted with the specific file and a manual control of the results is carried out before forwarding any result to the investigating officer. The biometric data is not forwarded outside of the controlled, isolated environment. Solely the result and the picture (not biometric template) is further used in the investigation. Employees receive specific training on the rules and procedures for this processing and all processing of personal and biometric data is sufficiently specified in national law.

Source of information:

- Types of data subjects:  suspects identified from the CCTV recordings
- Source of image:  publicly accessible spaces  internet
- Connection to crime:  Direct temporal
  - Direct geographical
- Mode of information capture:  remote
- Context - affecting other fundamental rights: Yes, namely :  Freedom of assembly  Freedom of speech  various: \_\_\_\_\_

Reference database (to which captured information is compared):

- Specificity:  specific databases related to crime area

Algorithm:

- Processing type:  1-many identification

Outcome:

- Impact:  Direct (e.g. the data subject is arrested, questioned)
- Automated decision:  NO

Legal analysis:

- Applicable legal framework :  Specific national law for this processing (facial recognition) for that competent authority

### 4.2. Applicable legal framework

In this scenario, it is specified in national law that biometric data may be used in conducting forensic analysis when strictly necessary for achieving the purpose of identifying suspects committing a serious crime through the matching of the pictures in the description database. The national law specifies which data that may be processed, as well as the procedures for preserving the integrity and

confidentiality of personal data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness.

#### 4.3. Necessity and proportionality

The use of facial recognition is clearly more time efficient than manual matching at the forensic level. The manual selection of images beforehand limits the interference compared to running all the video material against a database and thereby differentiates and targets only those persons covered by the objective, i.e. fighting serious crime. It is however still important to consider whether the matching can be done manually within a reasonable amount of time, depending on the case at hand. The restriction of persons with access to the technology and the personal data lessens the impact on the rights to privacy and data protection, as well as the biometric templates not being stored or used later on in the investigation. The manual control of the result also means a reduced risk of any false positives.

#### 4.4. Conclusion

It is important that national legislation provides an adequate legal basis for the processing of biometric data as well as for the national data base to which the matching takes place. In this scenario several measures have been put in place in order to limit the interference with data protection rights, such as the conditions for the use of the FRT specified in the legal basis, the number of people with access to the technology and the biometric data, manual controls etc. The FRT significantly improves efficiency in the investigatory work of the forensic department of the police, is based on law allowing for the police to process biometric data when absolutely necessary and therefore, within these perimeters may be considered a lawful interference of the rights of the individual.

### 5 SCENARIO 5

#### 5.1. Description

Remote biometric identification is when the identities of persons are established with the help of biometric identifiers (facial image, gait, iris, etc.) at a distance, in a public space and in a continuous or ongoing manner by checking them against (biometric) data stored in a database<sup>89</sup>. Remote biometric identification is conducted in real-time, if the capturing of the image material, the comparison and the identification happen with no significant delay.

Prior to each deployment of real time remote biometric identification, the police compiles a watch list of subjects of interest as part of an investigation. It is populated with facial images of the individuals. Based on intelligence suggesting that the individuals will be in a specific area, such as a shopping mall or a public square, the police decides when, where and for how long to deploy the remote biometric identification.

On the action day, they place a police van on the ground as a control centre, with a senior police officer on board. The van contains monitors displaying footage from CCTV cameras sited nearby, either installed on an ad-hoc basis or by connecting to the video streams of cameras already installed. As pedestrians pass by the cameras, the technology isolates facial images, converts them to a biometric template and compares these to the biometric templates of those on the watch list.

If a potential match between the watch list and those passing the cameras is detected, an alert is sent to officers in the van, who then advise officers on the ground if the alert is positive, e.g. via radio device. The officer on the ground will then decide whether to intervene, approach or ultimately apprehend

---

<sup>89</sup> [https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020\\_en.pdf](https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf)

the individual. The measures taken by the officer on the ground are recorded. In the case of a discreet check, the information gathered (such as who the person is with, what they are wearing and where they are heading to) is stored.

A national law referred to provides for a generic provision, according to which the processing of biometric data for the purpose of uniquely identifying a natural person is admissible if strictly necessary and subject to appropriate safeguards for the rights and freedoms of the person concerned.

Source of information:

- Types of data subjects:  all persons
- Source of image:  publicly accessible spaces
- Connection to crime:  Not necessarily direct geographical or temporal connection
- Mode of information capture:  remote
- Context - affecting other fundamental rights: Yes, namely:  Freedom of assembly  Freedom of speech  various
- Available additional sources of information about the data subject:  
 other: not excluded (such as usage of ATM-machines or shops entered)

Reference database (to which captured information is compared):

- Specificity:  specific databases related to crime area

Algorithm:

- Processing type:  1-many identification

Outcome:

- Impact:  Direct (e.g. the data subject is arrested, questioned)
- Automated decision:  NO
- Duration of storage: until all possible investigations are terminated

Legal analysis:

- Type of prior information to data subject:  In the LEA's website in general
- Applicable legal framework:  LED mostly copied to national law  Generic national law for the use of biometric data by LEAs

## 5.2. Applicable legal framework

Legal bases merely repeating the general clause of Article 10 LED are not sufficiently clear in their terms to give individuals an adequate indication of conditions and circumstances in which LEAs are empowered to use CCTV recordings from public spaces for creating a biometric template of their face and compare it to police databases. The legal framework established in this scenario therefore fails to meet the minimum requirements to serve as a legal base.<sup>90</sup>

## 5.3. Necessity and proportionality

The bar for necessity and proportionality becomes higher the deeper the interference. There are several fundamental rights implications of remote biometric identification in public spaces:

---

<sup>90</sup> In cases where a scientific project aiming at researching the use of FRT would need to process personal data, but such processing would not fall under Article 4 (3)LED or outside the scope of Union law, the GDPR would be applicable. In case of pilot projects that would be followed by law enforcement operations, the LED would still be applicable.

The scenarios entail the monitoring of every passers-by in the respective public space. Thus, it severely affects the populations' reasonable expectation of being anonymous in public spaces<sup>91</sup>. This is a prerequisite for many facets of the democratic process, such as the decision to join a civic association, visit gatherings and meet people of all social and cultural backgrounds, participate in a political protest and visit places of all kinds. The notion of anonymity in public spaces is essential to gather and exchange information and ideas freely. It preserves the plurality of opinion, the freedom of peaceful assembly and freedom of association and the protection of minorities and supports the principles of separation of powers and checks and balances. Undermining the notion of anonymity in public spaces can result in a severe chilling effect on citizens. They may refrain from certain behaviours which are well within the remits of a free and open society. This would affect the public interest, as a democratic society requires the self-determination and participation of its citizens in the democratic process.

If such a technology is applied, simply to walk on the street, to the subway or to the bakery in the affected area will lead to the collection of personal, including biometric data by law enforcement agencies and, in the first scenario, also to matching with police databases. A situation, where the same would be done by taking fingerprints, would be clearly disproportionate.

The number of data subjects affected is extremely high, since everyone walking past the respective public area is affected. Furthermore, the scenarios would imply automated mass processing of biometric data, and also a mass matching of biometric data against police databases.

Across European case law, mass surveillance is prohibited (e.g. the ECtHR in *S. and Marper v UK* considered the indiscriminate retention of biometric data as a "disproportionate interference" with the right to privacy, as it fails to be regarded "necessary in a democratic society").

Remote biometric identification is so prone to mass surveillance that there are no reliable means of restriction. It is essentially different from video surveillance as such, as the possible use of video footage without biometric identification is already a strong interference, but at the same time limited, whereas if FRT is applied, the already wide-spread video surveillance system as the main source of the data will undergo a change of quality. Moreover, especially with regard to the chilling effects implied, possible restrictions in the application of the already existing video surveillance installations will not be visible and thus not trusted by the public.

Remote biometric identification by police authorities treats everyone as a potential suspect. In a state under the rule of law, however, citizens are presumed to be righteous until misconduct can be proven. This principle is also partly reflected in the LED, which underlines the need for distinction, in so far as possible, between the treatment of criminal convicts or suspects in which case law enforcement must have "*serious grounds for believing that they have committed or are about to commit a criminal offence*" (Article 6(a) LED) compared to those who are not convicted or suspected of criminal activity.

Applied to transport nodal points or public spaces, with law enforcement agencies using a technology able to uniquely identify a single person, and to trace and analyse its whereabouts and movements will reveal up to the most sensitive information about a person (even sexual preferences, religion, health problems). With this comes the immense risk of unlawful access and use of the data.

The installation of a system that enables uncovering the very core of the individual's behaviour and characteristics leads to strong chilling effects. It makes people question whether to join a certain manifestation, thus damaging the democratic process. Also meeting and being seen in public with a

---

<sup>91</sup> EDPB response to MEPs, concerning the facial recognition app developed by Clearview AI, 10 June 2020, Ref: OUT2020-0052.

certain friend known as having trouble with police or behaving in a unique way might be seen as critical, since all of this would lead to the attraction of the system's algorithm and thus of law enforcement.

It is impossible to protect vulnerable data subjects like children. Moreover, persons who have a professional interest in – and often a corresponding legal obligation to – keeping their contacts confidential, such as journalists, lawyers and clergy, are affected. This could e.g. lead to the revelation of the source and the journalist, or the fact that a person consults a criminal defence attorney. The problem does not only apply to random public places, where e.g. journalists and their sources meet, but naturally also to public spaces necessary to approach and access institutions or professionals in this regard.

Furthermore, people's discomfort with FRT may lead them to changing their behaviour, avoiding places where FRT is deployed and thus withdrawing from social life and cultural events. Depending on the extent of the FRT deployment, the impact on people may be so significant as to affect their capacity to live a dignified life<sup>92</sup>.

Therefore, there is a strong likelihood to affect the essence – the untouchable core – of the right to protection of personal data. Strong indications (cf. section 3.1.3.2 of the guidelines) are in particular the following: on a large scale, people's unique biological features are automatically processed by law enforcement authorities with algorithms based on plausibility with only a limited explainability of the results. The limitations to the rights to privacy and data protection are imposed irrespective of the person's individual conduct or the circumstances concerning him or her. Statistically almost all of the data subjects affected by this interference are law-abiding individuals. There are only limited possibilities of providing information to the data subject. Judicial recourse in most cases will only be possible subsequently.

The reliance on a system based on plausibility and with limited explainability may lead to diffusion of liability and a lack in the field of remedy and may be an incentive towards negligence.

Once such a system, that may be applied also to existing CCTV cameras, is applied, with very little effort and without being visible to the individuals, it may be misused and enabled to systematically and speedily draw up lists of people according to ethnic origin, sex, religion etc. The principle of processing personal data against pre-determined criteria such as a person's whereabouts and the route travelled is already practiced<sup>93</sup> and is prone to discrimination.

Corresponding to the sensitivity, the expressiveness and the quantity of data processed, systems for remote facial recognition in publicly accessible places are prone to be misused with detrimental effects for the concerned individuals. Such data may also be easily collected and misused to put pressure on key actors in the principle of checks and balances such as political opposition, officers and journalists.

---

<sup>92</sup> [https://fra.europa.eu/sites/default/files/fra\\_uploads/fra-2019-facial-recognition-technology-focus-paper-1\\_en.pdf](https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf), page 20.

<sup>93</sup> C.f. Article 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 and Article 33 Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226.

Lastly, FRT-systems tend to incorporate strong bias effects regarding race and gender: false-positive results disproportionately affect people of colour and women<sup>94</sup>, resulting in discrimination. Police measures following a false-positive result, such as searches and arrests, stigmatise these groups further.

#### 5.4. Conclusion

The aforementioned scenarios concerning remote processing of biometric data in public spaces for identification purposes fail to strike a fair balance between the competing private and public interests, thus constituting a disproportionate interference with the data subject's rights under Articles 7 and 8 of the Charter.

## 6 SCENARIO 6

### 6.1. Description

A private entity provides an application where facial images are scraped off the internet to create a database. The user, e.g. the police, can then upload a picture and by using biometric identification the application will try to match it with the facial images or biometric templates in its database.

A local police department is conducting an investigation of a crime caught on video where a number of potential witnesses and suspects cannot be identified through matching collected information with any internal databases or intelligence. The individuals are, based on the information collected, not registered in any existing police database. The police decides to use a tool as described above, which is provided by a private company, to identify the individuals through biometric identification.

Source of information:

- Types of data subjects:  all citizens (witnesses)  convicts  suspects
- Source of image:  Video footage from a public place or collected elsewhere within a preliminary investigation
- Connection to crime:  Not necessary
- Mode of information capture:  remote
- Context - affecting other fundamental rights: Yes, namely:  Freedom of assembly  Freedom of speech  various: \_\_\_\_\_

Reference database (to which captured information is compared):

- Specificity:  general purpose databases populated from internet

Algorithm:

- Processing type:  1 - many identification

Outcome:

- Impact  Direct (e.g. the data subject is arrested, questioned, discriminatory behavior)
- Automated decision:  NO

Legal analysis:

- Type of prior information to data subject:  No

---

<sup>94</sup> <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>, <http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>

## 6.2. Applicable legal framework

When a private entity provides a service that includes personal data processing for which they determine the purpose and means (in this case scraping images off the internet to create a database), this private entity must have a legal basis for this processing. Furthermore, the law enforcement authority that decides to use this service for their purposes must have a legal basis for the processing for which they determine the purposes and means. For the law enforcement authority to be able to process biometric data, there has to be a legal framework that specifies the objective, the personal data to be processed, the purposes of the processing and the procedures for preserving the integrity and confidentiality of personal data as well as procedures for its destruction.

This scenario implies mass-scale collection of personal data from individuals not aware of their data being collected. Such processing could be lawful only under very exceptional circumstances. Depending on where the database is located using such a service may entail transferring personal data and/or special categories of personal data outside the European Union (by the police, e.g. "sending" the facial image in the surveillance video or collected otherwise), thereby requiring specific conditions for that transfer, see Article 39 LED.

There are no specific rules in this scenario that allow this processing by the law enforcement authority.

## 6.3. Necessity and proportionality

The law enforcement authority's use of the service means that personal data is shared with a private entity that is using a database where personal data is collected in an unlimited, mass-scale way. There is no connection between the personal data collected and the pursued objective by the law enforcement authority. The sharing of data by the law enforcement authority to the private entity also means a lack of control for the authority over the data being processed by the private entity and great difficulty for data subjects to exercise their rights, as they will not be aware of their data being processed in this way. This sets a very high bar for situations when such a processing could even take place. It is questionable if any objective would meet the requirements set out in the Directive, since any derogations from, and limitations to, the rights to privacy and data protection are only applicable when strictly necessary. The general interest of effectiveness in fighting serious crimes cannot in itself justify processing where such vast amounts of data are being collected indiscriminately. This processing would therefore not meet the requirements for necessity and proportionality.

## 6.4. Conclusion

The lack of clear, precise and foreseeable rules that meet the requirements in Articles 4 and 10 of the Directive, and the lack of evidence that this processing is strictly necessary in order to achieve the intended objectives, leads to the conclusion that the use of this application would not meet the necessity and proportionality requirements and would mean a disproportionate interference of data subjects' rights to respect for private life and the protection of personal data under the Charter.

# Guidelines



**Guidelines 2/2018 on derogations of Article 49 under  
Regulation 2016/679**

**Adopted on 25 May 2018**

## Contents

1. GENERAL.....	3
2. SPECIFIC INTERPRETATION OF THE PROVISIONS OF ARTICLE 49 .....	6
2.1 The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards - Article (49 (1) (a)) .....	6
2.1.1 Consent must be explicit .....	6
2.1.2 Consent must be specific for the particular data transfer/set of transfers .....	7
2.1.3 Consent must be informed particularly as to the possible risks of the transfer .....	7
2.2 Transfer necessary for the performance of a contract between the data subject and the controller or for the implementation of precontractual measures taken at the data subject's request - (49 (1) (b)) .....	8
2.3 Transfer necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person - (49 (1) (c)) .....	9
2.4 Transfer is necessary for important reasons of public interest - (49 (1) (d)) .....	10
2.5 Transfer is necessary for the establishment, exercise or defense of legal claims - (49 (1) (e)) ..	11
2.6 Transfer necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent – (49 (1) (f)) ..	12
2.7. Transfer made from a public register - (49 (1) (g) and 49 (2)) .....	13
2.8. Compelling legitimate interests – (49 (1) § 2) .....	14

# The European Data Protection Board

Having regard to Article 70 (1j) and (1e) 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,

## HAS ADOPTED FOLLOWING GUIDELINES:

### 1. GENERAL

This document seeks to provide guidance as to the application of Article 49 of the General Data Protection Regulation (GDPR)<sup>1</sup> on derogations in the context of transfers of personal data to third countries.

The document builds on the previous work<sup>2</sup> done by the Working Party of EU Data Protection Authorities established under Article 29 of the Data Protection Directive (the WP29) which is taken over by the European Data Protection Board (EDPB) regarding central questions raised by the application of derogations in the context of transfers of personal data to third countries. This document will be reviewed and if necessary updated, based on the practical experience gained through the application of the GDPR.

When applying Article 49 one must bear in mind that according to Article 44 the data exporter transferring personal data to third countries or international organizations must also meet the conditions of the other provisions of the GDPR. Each processing activity must comply with the relevant data protection provisions, in particular with Articles 5 and 6. Hence, a two-step test must be applied: first, a legal basis must apply to the data processing as such together with all relevant provisions of the GDPR; and as a second step, the provisions of Chapter V must be complied with.

Article 49 (1) states that in the absence of an adequacy decision or of appropriate safeguards, a transfer or a set of transfers of personal data to a third country or an international organization shall take place only under certain conditions. At the same time, Article 44 requires all provisions in Chapter V to be applied in such a way as to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined. This also implies that recourse to the derogations of Article 49 should never lead to a situation where fundamental rights might be breached.<sup>3</sup>

The WP29, as predecessor of the EDPB, has long advocated as best practice a layered approach<sup>4</sup> to transfers of considering first whether the third country provides an adequate level of protection and ensuring that the exported data will be safeguarded in the third country. If the level of protection is not adequate in light of all the circumstances, the data exporter should consider providing adequate

---

<sup>1</sup> 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).

<sup>2</sup> Article 29 Working Party, Working Document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, November 25,2005 (WP114)

<sup>3</sup>Article 29 Working Party, WP 114, p.9, and Article 29 Working Party Working Document on surveillance of electronic communications for intelligence and national security purposes (WP228), p.39.

<sup>4</sup> Article 29 Working Party, WP114, p.9

safeguards. Hence, data exporters should first endeavor possibilities to frame the transfer with one of the mechanisms included in Articles 45 and 46 GDPR, and only in their absence use the derogations provided in Article 49 (1).

Therefore, derogations under Article 49 are exemptions from the general principle that personal data may only be transferred to third countries if an adequate level of protection is provided for in the third country or if appropriate safeguards have been adduced and the data subjects enjoy enforceable and effective rights in order to continue to benefit from their fundamental rights and safeguards.<sup>5</sup> Due to this fact and in accordance with the principles inherent in European law,<sup>6</sup> the derogations must be interpreted restrictively so that the exception does not become the rule.<sup>7</sup> This is also supported by the wording of the title of Article 49 which states that derogations are to be used for specific situations (“Derogations for specific situations”).

When considering transferring personal data to third countries or international organizations, data exporters should therefore favour solutions that provide data subjects with a guarantee that they will continue to benefit from the fundamental rights and safeguards to which they are entitled as regards processing of their data once this data has been transferred. As derogations do not provide adequate protection or appropriate safeguards for the personal data transferred and as transfers based on a derogation are not required to have any kind of prior authorisation from the supervisory authorities, transferring personal data to third countries on the basis of derogations leads to increased risks for the rights and freedoms of the data subjects concerned.

Data exporters should also be aware that, in the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly limit transfers of specific categories of personal data to a third country or an international organization (Article 49 (5)).

### **Occasional and not repetitive transfers**

The EDPB notes that the term “occasional” is used in recital 111 and the term “not repetitive” is used in the “compelling legitimate interests” derogation under Article 49 par. 1 §2. These terms indicate that such transfers may happen more than once, but not regularly, and would occur outside the regular course of actions, for example, under random, unknown circumstances and within arbitrary time intervals. For example, a data transfer that occurs regularly within a stable relationship between the data exporter and a certain data importer can basically be deemed as systematic and repeated and can therefore not be considered occasional or not-repetitive. Besides, a transfer will for example generally be considered to be non-occasional or repetitive when the data importer is granted direct access to a database (e.g. via an interface to an IT-application) on a general basis.

Recital 111 differentiates among the derogations by expressly stating that the “contract” and the “legal claims” derogations (Article 49 (1) subpar. 1 (b), (c) and (e)) shall be limited to “occasional” transfers,

---

<sup>5</sup> Recital 114

<sup>6</sup> Article 29 Working Party, WP114, p.7

<sup>7</sup> See already Article 29 Working Party, WP114, pg. 7. The European Court of Justice repeatedly underlined that “the protection of the fundamental right to respect for private life at EU level requires that derogations from and limitations on the protection of personal data should apply only in so far as is strictly necessary” (judgments of 16 December 2008, Satakunnan Markkinapörssi and Satamedia, C 73/07, paragraph 56; of 9 November 2010, Volker und Markus Schecke and Eifert, C 92/09 and C 93/09, paragraph 77; the Digital Rights judgment, paragraph 52, and of 6 October 2015, Schrems, C 362/14, paragraph 92, and of 21 December 2016, Tele2 Sverige AB, C 203/15, paragraph 96). See also report on the Additional Protocol to Convention 108 on the control authorities and cross border flows of data, Article 2(2) (a), p.6 accessible at <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/181.1>

while such limitation is absent from the “explicit consent derogation”, the “important reasons of public interest derogation”, the “vital interests derogation” and the “register derogation” pursuant to Article 49 (1) subparagraph 1 (a), (d), (f) and, respectively, (g).

Nonetheless, it has to be highlighted that even those derogations which are not expressly limited to “occasional” or “not repetitive” transfers have to be interpreted in a way which does not contradict the very nature of the derogations as being exceptions from the rule that personal data may not be transferred to a third country unless the country provides for an adequate level of data protection or, alternatively, appropriate safeguards are put in place.<sup>8</sup>

### **Necessity test**

One overarching condition for the use of several derogations is that the data transfer has to be “necessary” for a certain purpose. The necessity test should be applied to assess the possible use of the derogations of Articles 49 (1) (b), (c), (d), (e) and (f). This test requires an evaluation by the data exporter in the EU of whether a transfer of personal data can be considered necessary for the specific purpose of the derogation to be used. For more information on the specific application of the necessity test in each of the concerned derogations, please refer to the relevant sections below.

### **Article 48 in relation to derogations**

The GDPR introduces a new provision in Article 48 that needs to be taken into account when considering transfers of personal data. Article 48 and the corresponding recital 115 provide that decisions from third country authorities, courts or tribunals are not in themselves legitimate grounds for data transfers to third countries. Therefore, a transfer in response to a decision from third country authorities is in any case only lawful, if in line with the conditions set out in Chapter V.<sup>9</sup>

In situations where there is an international agreement, such as a mutual legal assistance treaty (MLAT), EU companies should generally refuse direct requests and refer the requesting third country authority to existing MLAT or agreement.

This understanding also closely follows Article 44, which sets an overarching principle applying to all provisions of Chapter V, in order to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined.

---

<sup>8</sup>See Recital 115 sentence 4

## 2. SPECIFIC INTERPRETATION OF THE PROVISIONS OF ARTICLE 49

2.1 The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards - Article (49 (1) (a))

The general conditions for consent to be considered as valid are defined in Articles 4 (11)<sup>10</sup> and 7 of the GDPR<sup>11</sup>. The WP29 provides guidance on these general conditions for consent in a separate document, which is endorsed by the EDPB.<sup>12</sup> These conditions also apply to consent in the context of Article 49 (1) (a). However, there are specific, additional elements required for consent to be considered a valid legal ground for international data transfers to third countries and international organizations as provided for in Article 49 (1) (a), and this document will focus on them.

Therefore, this section (1) of the present guidelines shall be read in conjunction with the WP29 guidelines on consent, endorsed by the EDPB, which provide a more detailed analysis on the interpretation of the general conditions and criteria of consent under the GDPR.<sup>13</sup> It should also be noted that, according to Article 49 (3), public authorities are not able to rely on this derogation in the exercise of their public powers.

Article 49 (1) (a) states that a transfer of personal data to a third country or an international organization may be made in the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, on the condition that '*the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards*'.

### 2.1.1 Consent must be explicit

According to Article 4 (11) of the GDPR, any consent should be freely given, specific, informed and unambiguous. On this very last condition, Article 49 (1) (a) is stricter as it requires "explicit" consent. This is also a new requirement in comparison to Article 26 (1) (a) of Directive 95/46/EC, which only required "unambiguous" consent. The GDPR requires explicit consent in situations where particular data protection risks may emerge, and so, a high individual level of control over personal data is required, as is the case for the processing of special category data (Article 9 (2) (a)) and automated decisions (Article 22 (2) (c)). Such particular risks also appear in the context of international data transfers.

For further guidance on the requirement of explicit consent, and for the other applicable requirements needed for consent to be considered valid, please refer to the WP29's Guidelines on Consent which are endorsed by the EDPB.<sup>14</sup>

---

<sup>10</sup> According to Article 4(11) of the GDPR, 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

<sup>11</sup> Also recitals 32, 33, 42 and 43 give further guidance on consent

<sup>12</sup> See Article 29 Working Party Guidelines on Consent under Regulation 2016/679 (WP259)

<sup>13</sup> Idem

<sup>14</sup> Idem

## 2.1.2 Consent must be specific for the particular data transfer/set of transfers

One of the requirements of valid consent is that it must be specific. In order to constitute a valid ground for a data transfer pursuant to Article 49 (1) (a), hence, consent needs to be specifically given for the particular data transfer or set of transfers.

The element “specific” in the definition of consent intends to ensure a degree of user control and transparency for the data subject. This element is also closely linked with the requirement that consent should be “informed”.

Since consent must be specific, it is sometimes impossible to obtain the data subject’s prior consent for a future transfer at the time of the collection of the data, e.g. if the occurrence and specific circumstances of a transfer are not known at the time consent is requested, the impact on the data subject cannot be assessed. As an example, an EU company collects its customers’ data for a specific purpose (delivery of goods) without considering transferring this data, at that time, to a third party outside the EU. However, some years later, the same company is acquired by a non-EU company which wishes to transfer the personal data of its customers to another company outside the EU. In order for this transfer to be valid on the grounds of the consent derogation, the data subject should give his/her consent for this specific transfer at the time when the transfer is envisaged. Therefore, the consent provided at the time of the collection of the data by the EU company for delivery purposes is not sufficient to justify the use of this derogation for the transfer of the personal data outside the EU which is envisaged later.

Therefore, 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. This requirement is also related to the necessity for consent to be informed. It is possible to obtain the specific consent of a data subject prior to the transfer and at the time of the collection of the personal data as long as this specific transfer is made known to the data subject and the circumstances of the transfer do not change after the specific consent has been given by the data subject. Therefore the data exporter must make sure that the requirements set out in section 1.3 below are also complied with.

## 2.1.3 Consent must be informed<sup>15</sup> particularly as to the possible risks of the transfer

This condition is particularly important since it reinforces and further specifies the general requirement of “informed” consent as applicable to any consent and laid down in Art. 4 (11).<sup>16</sup> As such, the general requirement of “informed” consent, requires, in the case of consent as a lawful basis pursuant to Article 6(1) (a) for a data transfer, that the data subject is properly informed in advance of the specific circumstances of the transfer, (i.e. the data controller’s identity, the purpose of the transfer, the type of data, the existence of the right to withdraw consent, the identity or the categories of recipients).<sup>17</sup>

In addition to this general requirement of “informed” consent, where personal data are transferred to a third country under Article 49 (1) (a), this provision requires data subjects to be also 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. 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 transfer and therefore if it is not supplied, the derogation will not apply.

---

<sup>15</sup> The general transparency requirements of Articles 13 and 14 of the GDPR should also be complied with. For more information see Guidelines on transparency under Regulation 2016/679 (WP 260)

<sup>16</sup> See Article 29 Working Party Guidelines on Consent under Regulation 2016/679 (WP259)

<sup>17</sup> Idem, page 13

The information provided to data subjects in order to obtain consent for the transfer of their personal data to third parties established in third countries should also specify all data recipients or categories of recipients, all countries to which the personal data are being transferred to, that the consent is the lawful ground for the transfer, and that the third country to which the data will be transferred does not provide for an adequate level of data protection based on a European Commission decision.<sup>18</sup> In addition, as mentioned above, information has to be given as to the possible risks for the data subject arising from the absence of adequate protection in the third country and the absence of appropriate safeguards. Such notice, which could be standardized, 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 country.

In the specific case where a transfer is performed after the collection of personal data from the data subject has been made, the data exporter should inform the data subject of the transfer and of its risks before it takes place so as to collect his explicit consent to the “proposed” transfer.

As shown by the analysis above, the GDPR sets a high threshold for the use of the derogation of consent. This high threshold, combined with the fact that the consent provided by a data subject can be withdrawn at any time, means that consent might prove not to be a feasible long term solution for transfers to third countries.

## 2.2 Transfer necessary for the performance of a contract between the data subject and the controller or for the implementation of precontractual measures taken at the data subject's request - (49 (1) (b))

In view of recital 111, data transfers on the grounds of this derogation may take place “*where the transfer is occasional and necessary in relation to a contract (...)*”<sup>19</sup>

In general, although the derogations relating to the performance of a contract may appear to be potentially rather broad, they are being limited by the criterions of “necessity” and of “occasional transfers”.

### Necessity of the data transfer

The “*necessity test*”<sup>20</sup> limits the number of cases in which recourse can be made to Article 49 (1) (b).<sup>21</sup> It requires a close and substantial connection between the data transfer and the purposes of the contract.

This derogation cannot be used for example when a corporate group has, for business purposes, centralized its payment and human resources management functions for all its staff in a third country as there is no direct and objective link between the performance of the employment contract and such transfer.<sup>22</sup> Other grounds for transfer as provided for in Chapter V such as standard contractual clauses or binding corporate rules may, however, be suitable for the particular transfer.

---

<sup>18</sup> The last mentioned requirement also stems from the duty to inform the data subjects (Article 13(1)(f), Article 14(1)(e))

<sup>19</sup> The criterion of “occasional” transfers is found in recital 111 and applies to the derogations of Article 49 (1) (b), (c) and (e).

<sup>20</sup> See also Article 29 Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217)

<sup>21</sup> The “necessity” requirement also can be found in the derogations set forth in Article 49 (1) (c) to (f).

<sup>22</sup> In addition it will not be seen as being occasional (see below).

On the other hand, the transfer by travel agents of personal data concerning their individual clients to hotels or to other commercial partners that would be called upon in the organization of these clients' stay abroad can be deemed necessary for the purposes of the contract entered into by the travel agent and the client, since, in this case, there is a sufficient close and substantial connection between the data transfer and the purposes of the contract (organization of clients' travel).

This derogation cannot be applied to transfers of additional information not necessary for the performance of the contract or, respectively, for the implementation of precontractual measures requested by the data subject<sup>23</sup>; for additional data other tools would hence be required.

#### Occasional transfers

Personal data may only be transferred under this derogation when this transfer is occasional.<sup>24</sup> It would have to be established on a case by case basis whether data transfers or a data transfer would be determined as "*occasional*" or "*non-occasional*".

A transfer here may be deemed occasional for example if personal data of a sales manager, who in the context of his/her employment contract travels to different clients in third countries, are to be sent to those clients in order to arrange the meetings. A transfer could also be considered as occasional if a bank in the EU transfers personal data to a bank in a third country in order to execute a client's request for making a payment, as long as this transfer does not occur in the framework of a stable cooperation relationship between the two banks.

On the contrary, transfers would not qualify as "*occasional*" in a case where a multi-national company organises trainings in a training centre in a third country and systematically transfers the personal data of those employees that attend a training course (e.g. data such as name and job title, but potentially also dietary requirements or mobility restrictions). Data transfers regularly occurring within a stable relationship would be deemed as systematic and repeated, hence exceeding an "*occasional*" character. Consequently, in this case many data transfers within a business relationship may not be based on Article 49 (1) (b).

According to Article 49(1) (3), this derogation cannot apply to activities carried out by public authorities in the exercise of their public powers.

### [2.3 Transfer necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person - \(49 \(1\) \(c\)\)](#)

The interpretation of this provision is necessarily similar to that of Article 49 (1) (b); namely, that a transfer of data to a third country or an international organization in the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, can only be deemed to fall under the derogation of Article 49(1) (c), if it can be considered to be "*necessary for the conclusion or performance of a contract between the data controller and another natural or legal person, in the interest of the data subject*".

Aside from being necessary, recital 111 indicates that, data transfers may only take place "*where the transfer is **occasional** and **necessary** in relation to a contract (...)*" Therefore, apart from the "*necessity*

---

<sup>23</sup> More generally, all derogations of Article 49(1) (b) to (f) only allow that the data which are necessary for the purpose of the transfer may be transferred.

<sup>24</sup> As to the general definition of the term « *occasional* » see page 4

*test*", personal data here as well may only be transferred under this derogation only when the transfer is occasional.

#### Necessity of the data transfer and conclusion of the contract in the interest of the data subject

Where an organization has, for business purposes, outsourced activities such as payroll management to service providers outside the EU, this derogation will not provide a basis for data transfers for such purposes, since no close and substantial link between the transfer and a contract concluded in the data subject's interest can be established even if the end purpose of the transfer is the management of the pay of the employee.<sup>25</sup> Other transfer tools provided in Chapter V may provide a more suitable basis for such transfers such as standard contractual clauses or binding corporate rules.

#### Occasional transfers

Moreover, personal data may only be transferred under this derogation, when the transfer is occasional as it is the case under the derogation of Article 49 (1) (b). Therefore, in order to assess whether such transfer is occasional, the same test has to be carried out<sup>26</sup>.

Finally, according to Article 49(1) (3), this derogation cannot apply to activities carried out by public authorities in the exercise of their public powers.<sup>27</sup>

### 2.4 Transfer is necessary for important reasons of public interest - (49 (1) (d))

This derogation, usually referred to as the "important public interest derogation", is very similar to the provision contained in Directive 95/46/EC<sup>28</sup> under Article 26 (1) (d), which provides that a transfer shall take place only where it is necessary or legally required on important public interest grounds.

According to Article 49 (4), only public interests recognized in Union law or in the law of the Member State to which the controller is subject can lead to the application of this derogation.

However, for the application of this derogation, it is not sufficient that the data transfer is requested (for example by a third country authority) for an investigation which serves a public interest of a third country which, in an abstract sense, also exists in EU or Member State law. Where for example a third country authority requires a data transfer for an investigation aimed at combatting terrorism, the mere existence of EU or member state legislation also aimed at combatting terrorism is not as such a sufficient trigger to apply Article 49 (1) (d) to such transfer. Rather, as emphasized by the WP29, predecessor of the EDPB, in previous statements,<sup>29</sup> the derogation only applies when it can also be deduced from EU law or the law of the member state to which the controller is subject that such data transfers are allowed for important public interest purposes including in the spirit of reciprocity for international cooperation. The existence of an international agreement or convention which recognises a certain objective and provides for international cooperation to foster that objective can be an indicator when assessing the existence of a public interest pursuant to Article 49 (1) (d), as long as the EU or the Member States are a party to that agreement or convention.

---

<sup>25</sup> In addition it will not be seen as being occasional (see below).

<sup>26</sup> As to the general definition of the term "occasional" please see page 4

<sup>27</sup> For more information please refer to section 1, page 5 above.

<sup>28</sup> 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

<sup>29</sup> Article 29 Working Party Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) (WP128), p. 25

Although mainly focused to be used by public authorities, Article 49 (1) (d) may also be relied upon by private entities. This is supported by some of the examples enumerated in recital 112 which mention both transfers by public authorities and private entities<sup>30</sup>.

As such, the essential requirement for the applicability of this derogation is the finding of an important public interest and not the nature of the organization (public, private or international organization) that transfers and/or receives the data.

Recitals 111 and 112 indicate that this derogation is not limited to data transfers that are “occasional”<sup>31</sup>. Yet, this does not mean that data transfers on the basis of the important public interest derogation under Article 49 (1) (d) 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 shall 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.<sup>32</sup>

Where transfers are made in the usual course of business or practice, the EDPB strongly encourages all data exporters (in particular public bodies<sup>33</sup>) to frame these by putting in place appropriate safeguards in accordance with Article 46 rather than relying on the derogation as per Article 49(1) (d).

## 2.5 Transfer is necessary for the establishment, exercise or defense of legal claims - (49 (1) (e))

### Establishment, exercise or defense of legal claims

Under Article 49 (1) (e), transfers may take place when “*the transfer is necessary for the establishment, exercise or defense of legal claims*”. Recital 111 states that a transfer can be made where it is “*occasional and necessary in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies*”. This covers a range of activities for example, in the context of a criminal or administrative investigation in a third country (e.g. anti-trust law, corruption, insider trading or similar situations), where the derogation may apply to a transfer of data for the purpose of defending oneself or for obtaining a reduction or waiver of a fine legally foreseen e.g. in anti-trust investigations. As well, data transfers for the purpose of formal pre-trial discovery procedures in civil litigation may fall under this derogation. It can also cover actions by the data exporter to institute procedures in a third country for example commencing litigation or seeking approval for a merger. The derogation cannot be used to justify the transfer of personal data on the grounds of the mere possibility that legal proceedings or formal procedures may be brought in the future.

This derogation can apply to activities carried out by public authorities in the exercise of their public powers (Article 49 (3)).

The combination of the terms “legal claim” and “procedure” implies that the relevant procedure must have a basis in law, including a formal, legally defined process, but is not necessarily limited to judicial or administrative procedures (“or any out of court procedure”). As a transfer needs to be made in a

---

<sup>30</sup> “international data exchange between competition authorities, tax or customs administrations, between financial supervisory authorities, between services competent for social security matters, or for public health, for example in the case of contact tracing for contagious diseases or in order to reduce and/or eliminate doping in sport.”

<sup>31</sup> As to the general definition of the term « occasional » see page 4

<sup>32</sup> See also page 3

<sup>33</sup> For example financial supervisory authorities exchanging data in the context of international transfers of personal data for administrative cooperation purposes

procedure, a close link is necessary between a data transfer and a specific procedure regarding the situation in question. The abstract applicability of a certain type of procedure would not be sufficient.

Data controllers and data processors need to be aware that national law may also contain so-called “blocking statutes”, prohibiting them from or restricting them in transferring personal data to foreign courts or possibly other foreign official bodies.

#### Necessity of the data transfer

A data transfer in question may only take place when it is **necessary** for the establishment, exercise or defense of the legal claim in question. This “*necessity test*” requires a close and substantial connection between the data in question and the specific establishment, exercise or defense of the legal position.<sup>34</sup> The mere interest of third country authorities or possible “good will” to be obtained from the third country authority as such would not be sufficient.

Whilst there may be a temptation for a data exporter to transfer all possibly relevant personal data in response to a request or for instituting legal procedures, this would not be in line with this derogation or with the GDPR more generally as this (in the principle of data minimization) emphasizes the need for personal data to be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

In relation to litigation proceedings the WP29, predecessor of the EDPB, has already set out a layered approach to the question of whether the personal data should be transferred, including the application of this principle. As a first step, there should be a careful assessment of whether anonymized data would be sufficient in the particular case. If this is not the case, then transfer of pseudonymized data could be considered. If it is necessary to send personal data to a third country, its relevance to the particular matter should be assessed before the transfer – so only a set of personal data that is actually necessary is transferred and disclosed.

#### Occasional transfer

Such transfers should only be made if they are occasional. For information on the definition of occasional transfers please see the relevant section on “occasional and “non-repetitive” transfers.<sup>35</sup> Data exporters would need to carefully assess each specific case.

### [2.6 Transfer necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent – \(49 \(1\) \(f\)\)](#)

The derogation of Article 49 (1) (f) obviously applies when data is transferred in the event of a medical emergency and where it is considered that such transfer is directly necessary in order to give the medical care required.

Thus, for example, it must be legally possible to transfer data (including certain personal data) if the data subject, whilst outside the EU, is unconscious and in need of urgent medical care, and only a exporter (e.g. his usual doctor), established in an EU Member State, is able to supply these data. In such cases the law assumes that the imminent risk of serious harm to the data subject outweighs data protection concerns.

---

<sup>34</sup> Recital 111: “necessary in relation to a contract or a legal claim.”

<sup>35</sup> Page 4

The transfer must relate to the individual interest of the data subject or to that of another person's and, when it bears on health data, it must be necessary for an essential diagnosis. Accordingly, this derogation cannot be used to justify transferring personal medical data outside the EU if the purpose of the transfer is not to treat the particular case of the data subject or that of another person's but, for example, to carry out general medical research that will not yield results until sometime in the future.

Indeed, the GDPR does not restrict the use of this derogation to the physical integrity of a person but also leaves room for example to consider the cases where the mental integrity of a person should be protected. In this case, the person concerned would also be incapable - physically or legally - of providing his/her consent for the transfer of his/her personal data. In addition, the concerned individual whose personal data are the subject of the transfer specifically must not be able to give his/her consent – physically or legally - to this transfer.

However, whenever the data subject has the ability to make a valid decision, and his/her consent can be solicited, then this derogation cannot apply.

For example, where the personal data is required to prevent eviction from a property, this would not fall under this derogation as, even though housing be considered as a vital interest, the person concerned can provide his/her consent for the transfer of his/her data.

This ability to make a valid decision can depend on physical, mental but also legal incapability. A legal incapability can encompass, without prejudice to national representation mechanisms, for example, the case of a minor. This legal incapability has to be proved, depending on the case, through either a medical certificate showing the mental incapability of the person concerned or through a governmental document confirming the legal situation of the person concerned.

Data transfers to an international humanitarian organization, necessary to fulfil a task under the Geneva Conventions or to comply with international humanitarian law applicable in armed conflict may also fall under Article 49 (1) (f), see recital 112. Again, in such cases the data subject needs to be physically or legally incapable of giving consent.

The transfer of personal data after the occurrence of natural disasters and in the context of sharing of personal information with entities and persons for the purpose of rescue and retrieval operations (for example, relatives of disaster victims as well as with government and emergency services), can be justified under this derogation. Such unexpected events (floods, earthquakes, hurricanes etc.) can warrant the urgent transfer of certain personal data to learn for example, the location and status of victims. In such situations it is considered that the data subject concerned is unable to provide his/her consent for the transfer of his/her data.

## 2.7. Transfer made from a public register - (49 (1) (g) and 49 (2))

Article 49 (1) (g) and Article 49 (2) allow the transfer of personal data from registers under certain conditions. A register in general is defined as a “*(written) record containing regular entries of items or details*” or as “*an official list or record of names or items*”<sup>36</sup>, where in the context of Article 49, a register could be in written or electronic form.

The register in question must, according to Union or Member State law, be intended to provide information to the public. Therefore, private registers (those in the responsibility of private bodies) are

---

<sup>36</sup> Merriam Webster Dictionary, <https://www.merriam-webster.com/dictionary/register> (22.01.2018); Oxford Dictionary <https://en.oxforddictionaries.com/definition/register> (22.01.2018).

outside of the scope of this derogation (for example private registers through which credit-worthiness is appraised).

The register must be open to consultation by either:

- (a) the public in general or
- (b) any person who can demonstrate a legitimate interest.

These could be, for example: registers of companies, registers of associations, registers of criminal convictions, (land) title registers or public vehicle registers.

In addition to the general requirements regarding the set-up of the registers themselves, transfers from these registers may only take place if and to the extent that, in each specific case, the conditions for consultation that are set forth by Union or Member State law are fulfilled (regarding these general conditions, see Article 49 (1) (g)).

Data controllers and data processors wishing to transfer personal data under this derogation need to be aware that a transfer cannot include the entirety of the personal data or entire categories of the personal data contained in the register (Article 49 (2)). Where a transfer is made from a register established by law and where it is to be consulted by persons having a legitimate interest, the transfer can only be made at the request of those persons or if they are recipients, taking into account of the data subjects' interests and fundamental rights<sup>37</sup>. On a case by case basis, data exporters, in assessing whether the transfer is appropriate, would always have to consider the interests and rights of the data subject.

Further use of personal data from such registers as stated above may only take place in compliance with applicable data protection law.

This derogation can also apply to activities carried out by public authorities in the exercise of their public powers (Article 49 (3)).

## 2.8. Compelling legitimate interests – (49 (1) § 2)

Article 49 (1) § 2 introduces a new derogation which was not previously included in the Directive. Under a number of specific, expressly enumerated conditions, personal data can be transferred if it is necessary for the purposes of compelling legitimate interests pursued by the data exporter.

This derogation is envisaged by the law as a last resort, as it will only apply where “*a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation is applicable*”.<sup>38</sup>

This layered approach to considering the use of derogations as a basis for transfers requires consideration of whether it is possible to use a transfer tool provided in Article 45 or 46 or one of the specific derogations set out in Article 49 (1) § 1, before resorting to the derogation of Article 49 (1) § 2. This can only be used in residual cases according to recital 113 and is dependent on a significant number of conditions expressly laid down by law. In line with the principle of accountability enshrined in the GDPR<sup>39</sup> the data exporter must be therefore able to demonstrate that it was neither possible to frame the data transfer by appropriate safeguards pursuant to Article 46 nor to apply one of the derogations as contained in Article 49 (1) § 1.

---

<sup>37</sup> Recital 111 of the GDPR

<sup>38</sup> Article 49 (1) § 2 GDPR

<sup>39</sup> Article 5 (2) and Article 24 (1)

This implies that the data exporter can demonstrate serious attempts in this regard, taking into account the circumstances of the data transfer. This may for example and depending on the case, include demonstrating verification of whether the data transfer can be performed on the basis of the data subjects' explicit consent to the transfer under Article 49 (1) (a). However, in some circumstances the use of other tools might not be practically possible. For example, some types of appropriate safeguards pursuant to Article 46 may not be a realistic option for a data exporter that is a small or medium-sized company.<sup>40</sup> This may also be the case for example, where the data importer has expressly refused to enter into a data transfer contract on the basis of standard data protection clauses (Article 46 (2) (c)) and no other option is available (including, depending on the case, the choice of a different "data importer") – see also the paragraph below on 'compelling' legitimate interest.

#### *Compelling legitimate interests of the controller*

According to the wording of the derogation, the transfer must be necessary for the purposes of pursuing compelling legitimate interests of the data controller which are not overridden by the interests or rights and freedoms of the data subject. Consideration of the interests of a data exporter in its capacity as data processor or of the data importer are not relevant.

Moreover, only interests that can be recognized as "compelling" are relevant and this considerably limits the scope of the application of the derogation as not all conceivable "legitimate interests" under Article 6 (1) (f) will apply here. Rather a certain higher threshold will apply, requiring the compelling legitimate interest to be essential for the data controller. For example, this might be the case if a data controller is compelled to transfer the personal data in order to protect its organization or systems from serious immediate harm or from a severe penalty which would seriously affect its business.

#### *Not repetitive*

According to its express wording, Article 49 (1) § 2 can only apply to a transfer that is not repetitive<sup>41</sup>.

#### *Limited number of data subjects*

Additionally, the transfer must only concern a limited number of data subjects. No absolute threshold has been set as this will depend on the context but the number must be appropriately small taking into consideration the type of transfer in question.

In a practical context, the notion "limited number of data subjects" is dependent on the actual case in hand. For example, if a data controller needs to transfer personal data to detect a unique and serious security incident in order to protect its organization, the question here would be how many employees' data the data controller would have to transfer in order to achieve this compelling legitimate interest.

As such, in order for the derogation to apply, this transfer should not apply to all the employees of the data controller but rather to a certain confined few.

#### *Balancing the "compelling legitimate interests of the controller" against the "interests or rights and freedoms of the data subject" on the basis of an assessment of all circumstances surrounding the data transfer and providing for suitable safeguards*

As a further requirement, a balancing test between the data exporter's (compelling) legitimate interest pursued and the interests or rights and freedoms of the data subject has to be performed. In this

---

<sup>40</sup> For example binding corporate rules may often not be a feasible option for small and medium-sized enterprises due to the considerable administrative investments they imply.

<sup>41</sup> For more information on the term « not repetitive » see page 4

regard, the law expressly requires the data exporter to assess all circumstances of the data transfer in question and, based on this assessment, to provide “suitable safeguards” regarding the protection of the data transferred. This requirement highlights the special role that safeguards may play in reducing the undue impact of the data transfer on the data subjects and thereby in possibly influencing the balance of rights and interests to the extent that the data controller’s interests will not be overridden.<sup>42</sup>

As to the interests, rights and freedoms of the data subject which need to be taken into consideration, the possible negative effects, i.e. the risks of the data transfer on any type of (legitimate) interest of the data subject have to be carefully forecasted and assessed, by taking into consideration their likelihood and severity.<sup>43</sup> In this regard, in particular any possible damage (physical and material, but also non-material as e.g. relating to a loss of reputation) needs to be taken into consideration<sup>44</sup>. When assessing these risks and what could under the given circumstances possibly be considered as “suitable safeguards” for the rights and freedoms of the data subject, the data exporter needs to particularly take into account the nature of the data, the purpose and duration of the processing as well as the situation in the country of origin, the third country and, if any, the country of final destination of the transfer.<sup>45</sup>

Furthermore, the law requires the data exporter to apply additional measures as safeguards in order to minimize the identified risks caused by the data transfer for the data subject.<sup>46</sup> This is set up by the law as a mandatory requirement, so it can be followed that in the absence of additional safeguards, the controller’s interests in the transfer will in any case be overridden by the interests or rights and freedoms of the data subject.<sup>47</sup> As to the nature of such safeguards, it is not possible to set up general requirements applicable to all cases in this regard, but these will rather very much depend on the specific data transfer in question. Safeguards might include, depending on the case, for example measures aimed at ensuring deletion of the data as soon as possible after the transfer, or limiting the purposes for which the data may be processed following the transfer. Particular attention should be paid to whether it may be sufficient to transfer pseudonymized or encrypted data.<sup>48</sup> Moreover, technical and organizational measures aimed at ensuring that the transferred data cannot be used for other purposes than those strictly foreseen by the data exporter should be examined.

#### Information of the supervisory authority

The duty to inform the supervisory authority does not mean that the transfer needs to be authorized by the supervisory authority, but rather it serves as an additional safeguard by enabling the supervisory

---

<sup>42</sup> The important role of safeguards in the context of balancing the interests of the data controller and the data subjects has already been highlighted by the Article 29 Working Party in WP 217, p. 31.

<sup>43</sup> See Recital 75: “*The risk to the rights and freedoms of natural persons, of varying likelihood and severity (...)*”

<sup>44</sup> See Recital 75: “*The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage.*”

<sup>45</sup> Recital 113

<sup>46</sup> While in the context of an “ordinary” balancing test foreseen by the law such (additional) measures might not be necessary in each case (see Article 29 Working Party Working document on Draft Ad hoc contractual clauses “EU data processor to non-EU sub-processor” (WP 214), p. 41), the wording of Art. 49 (1) § 2 suggests that additional measures are mandatory in order the data transfer to comply with the “balancing test” and therefore to be feasible under this derogation.

<sup>47</sup> While in the context of an “ordinary” balancing test foreseen by the law such (additional) measures might not be necessary in each case (see Article 29 Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, p. 41), the wording of Art. 49 (1) § 2 suggests that additional measures are mandatory in order the data transfer to comply with the “balancing test” and therefore to be feasible under this derogation.

<sup>48</sup> For other examples of possible safeguards see Article 29 Working Party Working document on Draft Ad hoc contractual clauses “EU data processor to non-EU sub-processor” (WP 214), p. 41-43

authority to assess the data transfer (if it considers it appropriate) as to its possible impact on the rights and freedoms of the data subjects affected. As part of its compliance with the accountability principle, it is recommended that the data exporter records all relevant aspects of the data transfer e.g. the compelling legitimate interest pursued, the “competing” interests of the individual, the nature of the data transferred and the purpose of the transfer.

*Providing information of the transfer and the compelling legitimate interests pursued to the data subject*

The data controller must inform the data subject of the transfer and of the compelling legitimate interests pursued. This information must be provided in addition to that required to be provided under Articles 13 and 14 of the GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

# Guidelines



## **Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)**

**Version 2.1**

**12 November 2019**

## Version history

Version 2.1	07 January 2020	Formatting change
Version 2.0	12 November 2019	Adoption of the Guidelines after public consultation
Version 1.0	16 November 2018	Adoption of the Guidelines for publication consultation

## **Contents**

Introduction .....	4
1 Application of the establishment criterion - Art 3(1).....	5
2 Application of the targeting criterion – Art 3(2) .....	13
3 Processing in a place where Member State law applies by virtue of public international law .....	22
4 Representative of controllers or processors not established in the Union.....	23

## The European Data Protection Board

Having regard to Article 70 (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.

### HAS ADOPTED THE FOLLOWING GUIDELINES:

## INTRODUCTION

The territorial scope of General Data Protection Regulation<sup>1</sup> (the GDPR or the Regulation) is determined by Article 3 of the Regulation and represents a significant evolution of the EU data protection law compared to the framework defined by Directive 95/46/EC<sup>2</sup>. In part, the GDPR confirms choices made by the EU legislator and the Court of Justice of the European Union (CJEU) in the context of Directive 95/46/EC. However, important new elements have been introduced. Most importantly, the main objective of Article 4 of the Directive was to define which Member State's national law is applicable, whereas Article 3 of the GDPR defines the territorial scope of a directly applicable text. Moreover, while Article 4 of the Directive made reference to the 'use of equipment' in the Union's territory as a basis for bringing controllers who were "not established on Community territory" within the scope of EU data protection law, such a reference does not appear in Article 3 of the GDPR.

Article 3 of the GDPR reflects the legislator's intention to ensure comprehensive protection of the rights of data subjects in the EU and to establish, in terms of data protection requirement, a level playing field for companies active on the EU markets, in a context of worldwide data flows.

Article 3 of the GDPR defines the territorial scope of the Regulation on the basis of two main criteria: the "establishment" criterion, as per Article 3(1), and the "targeting" criterion as per Article 3(2). Where one of these two criteria is met, the relevant provisions of the GDPR will apply to relevant processing of personal data by the controller or processor concerned. In addition, Article 3(3) confirms the application of the GDPR to the processing where Member State law applies by virtue of public international law.

Through a common interpretation by data protection authorities in the EU, these guidelines seek to ensure a consistent application of the GDPR when assessing whether particular processing by a controller or a processor falls within the scope of the new EU legal framework. In these guidelines, the EDPB sets out and clarifies the criteria for determining the application of the territorial scope of the GDPR. Such a common interpretation is also essential for controllers and processors, both within and outside the EU, so that they may assess whether they need to comply with the GDPR for a given processing activity.

As controllers or processors not established in the EU but engaging in processing activities falling within Article 3(2) are required to designate a representative in the Union, these guidelines will also provide

---

<sup>1</sup> 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).

<sup>2</sup> 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.

clarification on the process for the designation of this representative under Article 27 and its responsibilities and obligations.

As a general principle, the EDPB asserts that where the processing of personal data falls within the territorial scope of the GDPR, all provisions of the Regulation apply to such processing. These guidelines will specify the various scenarios that may arise, depending on the type of processing activities, the entity carrying out these processing activities or the location of such entities, and will detail the provisions applicable to each situation. It is therefore essential that controllers and processors, especially those offering goods and services at international level, undertake a careful and *in concreto* assessment of their processing activities, in order to determine whether the related processing of personal data falls under the scope of the GDPR.

The EDPB underlines that the application of Article 3 aims at determining whether a particular processing activity, rather than a person (legal or natural), falls within the scope of the GDPR. Consequently, certain processing of personal data by a controller or processor might fall within the scope of the Regulation, while other processing of personal data by that same controller or processor might not, depending on the processing activity.

These guidelines, initially adopted by the EDPB on 16 November, have been submitted to a public consultation from 23<sup>rd</sup> November 2018 to 18<sup>th</sup> January 2019 and have been updated taking into account the contributions and feedback received.

## 1 APPLICATION OF THE ESTABLISHMENT CRITERION - ART 3(1)

Article 3(1) of the GDPR provides that the “*Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.*”

Article 3(1) GDPR makes reference not only to an establishment of a controller, but also to an establishment of a processor. As a result, the processing of personal data by a processor may also be subject to EU law by virtue of the processor having an establishment located within the EU.

Article 3(1) ensures that the GDPR applies to the processing by a controller or processor carried out in the context of the activities of an establishment of that controller or processor in the Union, regardless of the actual place of the processing. The EDPB therefore recommends a threefold approach in determining whether or not the processing of personal data falls within the scope of the GDPR pursuant to Article 3(1).

The following sections clarify the application of the establishment criterion, first by considering the definition of an ‘establishment’ in the EU within the meaning of EU data protection law, second by looking at what is meant by ‘processing in the context of the activities of an establishment in the Union’, and lastly by confirming that the GDPR will apply regardless of whether the processing carried out in the context of the activities of this establishment takes place in the Union or not.

### a) “An establishment in the Union”

Before considering what is meant by “an establishment in the Union” it is first necessary to identify who is the controller or processor for a given processing activity. According to the definition in Article 4(7) of the GDPR, controller means “the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data”. A processor, according to Article 4(8) of the GDPR, is “a natural or legal person, public authority,

agency or other body which processes personal data on behalf of the controller". As established by relevant CJEU case law and previous WP29 opinion<sup>3</sup>, the determination of whether an entity is a controller or processor for the purposes of EU data protection law is a key element in the assessment of the application of the GDPR to the personal data processing in question.

While the notion of "main establishment" is defined in Article 4(16), the GDPR does not provide a definition of "establishment" for the purpose of Article 3<sup>4</sup>. However, Recital 22<sup>5</sup> clarifies that an "[e]stablishment implies the effective and real exercise of activities through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect."

This wording is identical to that found in Recital 19 of Directive 95/46/EC, to which reference has been made in several CJEU rulings broadening the interpretation of the term "establishment", departing from a formalistic approach whereby undertakings are established solely in the place where they are registered<sup>6</sup>. Indeed, the CJEU ruled that the notion of establishment extends to any real and effective activity — even a minimal one — exercised through stable arrangements<sup>7</sup>. In order to determine whether an entity based outside the Union has an establishment in a Member State, both the degree of stability of the arrangements and the effective exercise of activities in that Member State must be considered in the light of the specific nature of the economic activities and the provision of services concerned. This is particularly true for undertakings offering services exclusively over the Internet<sup>8</sup>.

The threshold for "stable arrangement"<sup>9</sup> can actually be quite low when the centre of activities of a controller concerns the provision of services online. As a result, in some circumstances, the presence of one single employee or agent of a non-EU entity in the Union may be sufficient to constitute a stable arrangement (amounting to an 'establishment' for the purposes of Art 3(1)) if that employee or agent acts with a sufficient degree of stability. Conversely, when an employee is based in the EU but the processing is not being carried out in the context of the activities of the EU-based employee in the Union (i.e. the processing relates to activities of the controller outside the EU), the mere presence of an employee in the EU will not result in that processing falling within the scope of the GDPR. In other words, the mere presence of an employee in the EU is not as such sufficient to trigger the application of the GDPR, since for the processing in question to fall within the scope of the GDPR, it must also be carried out in the context of the activities of the EU-based employee.

The fact that the non-EU entity responsible for the data processing does not have a branch or subsidiary in a Member State does not preclude it from having an establishment there within the

---

<sup>3</sup> G 29 WP169 - Opinion 1/2010 on the concepts of "controller" and "processor", adopted on 16<sup>th</sup> February 2010 and under revision by the EDPB.

<sup>4</sup> The definition of "main establishment" is mainly relevant for the purpose of determining the competence of the supervisory authorities concerned according to Article 56 GDPR. See the WP29 Guidelines for identifying a controller or processor's lead supervisory authority (16/EN WP 244 rev.01) - endorsed by the EDPB.

<sup>5</sup> Recital 22 of the GDPR: "Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect."

<sup>6</sup> See in particular *Google Spain SL, Google Inc. v AEPD, Mario Costeja González (C-131/12)*, *Weltimmo v NAIH (C-230/14)*, *Verein für Konsumenteninformation v Amazon EU (C-191/15)* and *Wirtschaftsakademie Schleswig-Holstein (C-210/16)*.

<sup>7</sup> Weltimmo, paragraph 31.

<sup>8</sup> Weltimmo, paragraph 29.

<sup>9</sup> Weltimmo, paragraph 31.

meaning of EU data protection law. Although the notion of establishment is broad, it is not without limits. It is not possible to conclude that the non-EU entity has an establishment in the Union merely because the undertaking's website is accessible in the Union<sup>10</sup>.

**Example 1:** A car manufacturing company with headquarters in the US has a fully-owned branch office located in Brussels overseeing all its operations in Europe, including marketing and advertisement.

The Belgian branch can be considered to be a stable arrangement, which exercises real and effective activities in light of the nature of the economic activity carried out by the car manufacturing company. As such, the Belgian branch could therefore be considered as an establishment in the Union, within the meaning of the GDPR.

Once it is concluded that a controller or processor is established in the EU, an *in concreto* analysis should then follow to determine whether the processing in question is carried out in the context of the activities of this establishment, in order to determine whether Article 3(1) applies. If a controller or processor established outside the Union exercises "a real and effective activity - even a minimal one" - through "stable arrangements", regardless of its legal form (e.g. subsidiary, branch, office...), in the territory of a Member State, this controller or processor can be considered to have an establishment in that Member State<sup>11</sup>. It is therefore important to consider whether the processing of personal data takes place "in the context of the activities of" such an establishment as highlighted in Recital 22.

### b) Processing of personal data carried out "in the context of the activities of" an establishment

Article 3(1) confirms that it is not necessary that the processing in question is carried out "by" the relevant EU establishment itself; the controller or processor will be subject to obligations under the GDPR whenever the processing is carried out "in the context of the activities" of its relevant establishment in the Union. The EDPB recommends that determining whether processing is being carried out in the context of an establishment of the controller or processor in the Union for the purposes of Article 3(1) should be carried out on a case-by-case basis and based on an analysis *in concreto*. Each scenario must be assessed on its own merits, taking into account the specific facts of the case.

The EDPB considers that, for the purpose of Article 3(1), the meaning of "*processing in the context of the activities of an establishment of a controller or a processor*" is to be understood in light of the relevant case law. On the one hand, with a view to fulfilling the objective of ensuring effective and complete protection, the meaning of "in the context of the activities of an establishment" cannot be interpreted restrictively<sup>12</sup>. On the other hand, the existence of an establishment within the meaning of the GDPR should not be interpreted too broadly to conclude that the existence of any presence in the EU with even the remotest links to the data processing activities of a non-EU entity will be sufficient to bring this processing within the scope of EU data protection law. Some commercial activity carried out by a non-EU entity within a Member State may indeed be so far removed from the processing of

---

<sup>10</sup> CJEU, Verein für Konsumenteninformation v. Amazon EU Sarl, Case C-191/15, 28 July 2016, paragraph 76 (hereafter "Verein für Konsumenteninformation").

<sup>11</sup> See in particular para 29 of the Weltimmo judgment, which emphasizes a flexible definition of the concept of 'establishment' and clarifies that 'the degree of stability of the arrangements and the effective exercise of activities in that other Member State must be interpreted in the light of the specific nature of the economic activities and the provision of services concerned.'

<sup>12</sup> Weltimmo, paragraph 25 and Google Spain, paragraph 53.

personal data by this entity that the existence of the commercial activity in the EU would not be sufficient to bring the data processing by the non-EU entity within the scope of EU data protection law<sup>13</sup>.

Consideration of the following two factors may help to determine whether the processing is being carried out by a controller or processor in the context of its establishment in the Union

*i) Relationship between a data controller or processor outside the Union and its local establishment in the Union*

The data processing activities of a data controller or processor established outside the EU may be inextricably linked to the activities of a local establishment in a Member State, and thereby may trigger the applicability of EU law, even if that local establishment is not actually taking any role in the data processing itself<sup>14</sup>. If a case by case analysis on the facts shows that there is an inextricable link between the processing of personal data carried out by a non-EU controller or processor and the activities of an EU establishment, EU law will apply to that processing by the non-EU entity, whether or not the EU establishment plays a role in that processing of data<sup>15</sup>.

*ii) Revenue raising in the Union*

Revenue-raising in the EU by a local establishment, to the extent that such activities can be considered as “inextricably linked” to the processing of personal data taking place outside the EU and individuals in the EU, may be indicative of processing by a non-EU controller or processor being carried out “in the context of the activities of the EU establishment”, and may be sufficient to result in the application of EU law to such processing<sup>16</sup>.

The EDPB recommends that non-EU organisations undertake an assessment of their processing activities, first by determining whether personal data are being processed, and secondly by identifying potential links between the activity for which the data is being processed and the activities of any presence of the organisation in the Union. If such a link is identified, the nature of this link will be key in determining whether the GDPR applies to the processing in question, and must be assessed *inter alia* against the two elements listed above.

**Example 2:** An e-commerce website is operated by a company based in China. The personal data processing activities of the company are exclusively carried out in China. The Chinese company has established a European office in Berlin in order to lead and implement commercial prospection and marketing campaigns towards EU markets.

In this case, it can be considered that the activities of the European office in Berlin are inextricably linked to the processing of personal data carried out by the Chinese e-commerce website, insofar as

---

<sup>13</sup> G29 WP 179 update - Update of Opinion 8/2010 on applicable law in light of the CJEU judgment in Google Spain, 16th December 2015

<sup>14</sup> CJEU, Google Spain, Case C-131/12

<sup>15</sup> G29 WP 179 update - Update of Opinion 8/2010 on applicable law in light of the CJEU judgment in Google Spain, 16<sup>th</sup> December 2015

<sup>16</sup> This may potentially be the case, for example, for any foreign operator with a sales office or some other presence in the EU, even if that office has no role in the actual data processing, in particular where the processing takes place in the context of the sales activity in the EU and the activities of the establishment are aimed at the inhabitants of the Member States in which the establishment is located (WP179 update).

the commercial prospection and marketing campaign towards EU markets notably serve to make the service offered by the e-commerce website profitable. The processing of personal data by the Chinese company in relation to EU sales is indeed inextricably linked to the activities of the European office in Berlin relating to commercial prospection and marketing campaign towards EU market. The processing of personal data by the Chinese company in connection with EU sales can therefore be considered as carried out in the context of the activities of the European office, as an establishment in the Union. This processing activity by the Chinese company will therefore be subject to the provisions of the GDPR as per its Article 3(1)".

**Example 3:** A hotel and resort chain in South Africa offers package deals through its website, available in English, German, French and Spanish. The company does not have any office, representation or stable arrangement in the EU.

In this case, in the absence of any representation or stable arrangement of the hotel and resort chain within the territory of the Union, it appears that no entity linked to this data controller in South Africa can qualify as an establishment in the EU within the meaning of the GDPR. Therefore the processing at stake cannot be subject to the provisions of the GDPR, as per Article 3(1).

However, it must be analysed *in concreto* whether the processing carried out by this data controller established outside the EU can be subject to the GDPR, as per Article 3(2).

c) Application of the GDPR to the establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not

As per Article 3(1), the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union triggers the application of the GDPR and the related obligations for the data controller or processor concerned.

The text of the GDPR specifies that the Regulation applies to processing in the context of the activities of an establishment in the EU "*regardless of whether the processing takes place in the Union or not*". It is the presence, through an establishment, of a data controller or processor in the EU and the fact that a processing takes place in the context of the activities of this establishment that trigger the application of the GDPR to its processing activities. The place of processing is therefore not relevant in determining whether or not the processing, carried out in the context of the activities of an EU establishment, falls within the scope of the GDPR.

**Example 4:** A French company has developed a car-sharing application exclusively addressed to customers in Morocco, Algeria and Tunisia. The service is only available in those three countries but all personal data processing activities are carried out by the data controller in France.

While the collection of personal data takes place in non-EU countries, the subsequent processing of personal data in this case is carried out in the context of the activities of an establishment of a data controller in the Union. Therefore, even though processing relates to personal data of data subjects who are not in the Union, the provisions of the GDPR will apply to the processing carried out by the French company, as per Article 3(1).

**Example 5:** A pharmaceutical company with headquarters in Stockholm has located all its personal data processing activities with regards to its clinical trial data in its branch based in Singapore.

In this case, while the processing activities are taking place in Singapore, that processing is carried out in the context of the activities of the pharmaceutical company in Stockholm i.e. of a data controller established in the Union. The provisions of the GDPR therefore apply to such processing, as per Article 3(1).

In determining the territorial scope of the GDPR, geographical location will be important under Article 3(1) with regard to the place of establishment of:

- the controller or processor itself (is it established inside or outside the Union?);
- any business presence of a non-EU controller or processor (does it have an establishment in the Union?)

However, geographical location is not important for the purposes of Article 3(1) with regard to the place in which processing is carried out, or with regard to the location of the data subjects in question.

The text of Article 3(1) does not restrict the application of the GDPR to the processing of personal data of individuals who are in the Union. The EDPB therefore considers that any personal data processing in the context of the activities of an establishment of a controller or processor in the Union would fall under the scope of the GDPR, regardless of the location or the nationality of the data subject whose personal data are being processed. This approach is supported by Recital 14 of the GDPR which states that “[t]he protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data.”

#### d) Application of the establishment criterion to controller and processor

As far as processing activities falling under the scope of Article 3(1) are concerned, the EDPB considers that such provisions apply to controllers and processors whose processing activities are carried out in the context of the activities of their respective establishment in the EU. While acknowledging that the requirements for establishing the relationship between a controller and a processor<sup>17</sup> does not vary depending on the geographical location of the establishment of a controller or processor, the EDPB takes the view that when it comes to the identification of the different obligations triggered by the applicability of the GDPR as per Article 3(1), the processing by each entity must be considered separately.

The GDPR envisages different and dedicated provisions or obligations applying to data controllers and processors, and as such, should a data controller or processor be subject to the GDPR as per Article 3(1), the related obligations would apply to them respectively and separately. In this context, the EDPB notably deems that a processor in the EU should not be considered to be an establishment of a data controller within the meaning of Article 3(1) merely by virtue of its status as processor on behalf of a controller.

The existence of a relationship between a controller and a processor does not necessarily trigger the application of the GDPR to both, should one of these two entities not be established in the Union.

An organisation processing personal data on behalf of, and on instructions from, another organisation (the client company) will be acting as processor for the client company (the controller). Where a processor is established in the Union, it will be required to comply with the obligations imposed on

---

<sup>17</sup> In accordance with Article 28, the EDPB recalls that processing activities by a processor on behalf of a controller 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, and that controllers shall only use processors providing sufficient guarantees to implement appropriate measures in such manner that processing will meet the requirement of the GDPR and ensure the protection of data subjects' rights.

processors by the GDPR (the ‘GDPR processor obligations’). If the controller instructing the processor is also located in the Union, that controller will be required to comply with the obligations imposed on controllers by the GDPR (the ‘GDPR controller obligations’). Processing activity which, when carried out by a controller, falls within the scope of the GDPR by virtue of Art 3(1) will not fall outside the scope of the Regulation simply because the controller instructs a processor not established in the Union to carry out that processing on its behalf.

*i) Processing by a controller established in the EU instructing a processor not established in the Union*

Where a controller subject to GDPR chooses to use a processor located outside the Union for a given processing activity, it will still be necessary for the controller to ensure by contract or other legal act that the processor processes the data in accordance with the GDPR. Article 28(3) provides that the processing by a processor shall be governed by a contract or other legal act. The controller will therefore need to ensure that it puts in place a contract with the processor addressing all the requirements set out in Article 28(3). In addition, it is likely that, in order to ensure that it has complied with its obligations under Article 28(1) – to use only a processor providing sufficient guarantees to implement measures in such a manner that processing will meet the requirements of the Regulation and protect the rights of data subjects – the controller may need to consider imposing, by contract, the obligations placed by the GDPR on processors subject to it. That is to say, the controller would have to ensure that the processor not subject to the GDPR complies with the obligations, governed by a contract or other legal act under Union or Member State law, referred to Article 28(3).

The processor located outside the Union will therefore become indirectly subject to some obligations imposed by controllers subject to the GDPR by virtue of contractual arrangements under Article 28. Moreover, provisions of Chapter V of the GDPR may apply.

**Example 6:** A Finnish research institute conducts research regarding the Sami people. The institute launches a project that only concerns Sami people in Russia. For this project the institute uses a processor based in Canada.

The The Finnish controller has a duty to only use processors that provide sufficient guarantees to implement appropriate measures in such manner that processing will meet the requirement of the GDPR and ensure the protection of data subjects’ rights. The Finnish controller needs to enter into a data processing agreement with the Canadian processor, and the processor’s duties will be stipulated in that legal act.

*ii) Processing in the context of the activities of an establishment of a processor in the Union*

Whilst case law provides us with a clear understanding of the effect of processing being carried out in the context of the activities of an EU establishment of the controller, the effect of processing being carried out in the context of the activities of an EU establishment of a processor is less clear.

The EDPB emphasises that it is important to consider the establishment of the controller and processor separately when determining whether each party is of itself ‘established in the Union’.

The first question is whether the controller itself has an establishment in the Union, and is processing in the context of the activities of that establishment. Assuming the controller is not considered to be processing in the context of its own establishment in the Union, that controller will not be subject to GDPR controller obligations by virtue of Article 3(1) (although it may still be caught by Article 3(2)). Unless other factors are at play, the processor’s EU establishment will not be considered to be an establishment in respect of the controller.

The separate question then arises of whether the processor is processing in the context of its establishment in the Union. If so, the processor will be subject to GDPR processor obligations under Article 3(1). However, this does not cause the non-EU controller to become subject to the GDPR controller obligations. That is to say, a “non-EU” controller (as described above) will not become subject to the GDPR simply because it chooses to use a processor in the Union.

By instructing a processor in the Union, the controller not subject to GDPR is not carrying out processing “in the context of the activities of the processor in the Union”. The processing is carried out in the context of the controller’s own activities; the processor is merely providing a processing service<sup>18</sup> which is not “inextricably linked” to the activities of the controller. As stated above, in the case of a data processor established in the Union and carrying out processing on behalf of a data controller established outside the Union and not subject to the GDPR as per Article 3(2), the EDPB considers that the processing activities of the data controller would not be deemed as falling under the territorial scope of the GDPR merely because it is processed on its behalf by a processor established in the Union. However, even though the data controller is not established in the Union and is not subject to the provisions of the GDPR as per Article 3(2), the data processor, as it is established in the Union, will be subject to the relevant provisions of the GDPR as per Article 3(1).

**Example 7:** A Mexican retail company enters into a contract with a processor established in Spain for the processing of personal data relating to the Mexican company’s clients. The Mexican company offers and directs its services exclusively to the Mexican market and its processing concerns exclusively data subjects located outside the Union.

In this case, the Mexican retail company does not target persons on the territory of the Union through the offering of goods or services, nor it does monitor the behaviour of person on the territory of the Union. The processing by the data controller, established outside the Union, is therefore not subject to the GDPR as per Article 3(2).

The provisions of the GDPR do not apply to the data controller by virtue of Art 3(1) as it is not processing personal data in the context of the activities of an establishment in the Union. The data processor is established in Spain and therefore its processing will fall within the scope of the GDPR by virtue of Art 3(1). The processor will be required to comply with the processor obligations imposed by the regulation for any processing carried out in the context of its activities.

When it comes to a data processor established in the Union carrying out processing on behalf of a data controller with no establishment in the Union for the purposes of the processing activity and which does not fall under the territorial scope of the GDPR as per Article 3(2), the processor will be subject to the following relevant GDPR provisions directly applicable to data processors:

- The obligations imposed on processors under Article 28 (2), (3), (4), (5) and (6), on the duty to enter into a data processing agreement, with the exception of those relating to the assistance to the data controller in complying with its (the controller’s) own obligations under the GDPR.
- The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law, as per Article 29 and Article 32(4).
- Where applicable, the processor shall maintain a record of all categories of processing carried out on behalf of a controller, as per Article 30(2).

---

<sup>18</sup> The offering of a processing service in this context cannot be considered either as an offer of a service to data subjects in the Union.

- Where applicable, the processor shall, upon request, cooperate with the supervisory authority in the performance of its tasks, as per Article 31.
- The processor shall implement technical and organisational measures to ensure a level of security appropriate to the risk, as per Article 32.
- The processor shall notify the controller without undue delay after becoming aware of a personal data breach, as per Article 33.
- Where applicable, the processor shall designate a data protection officer as per Articles 37 and 38.
- The provisions on transfers of personal data to third countries or international organisations, as per Chapter V.

In addition, since such processing would be carried out in the context of the activities of an establishment of a processor in the Union, the EDPB recalls that the processor will have to ensure its processing remains lawful with regards to other obligations under EU or national law. Article 28(3) also specifies that "*the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.*"

In line with the positions taken previously by the Article 29 Working Party, the EDPB takes the view that the Union territory cannot be used as a "data haven", for instance when a processing activity entails inadmissible ethical issues<sup>19</sup>, and that certain legal obligations beyond the application of EU data protection law, in particular European and national rules with regard to public order, will in any case have to be respected by any data processor established in the Union, regardless of the location of the data controller. This consideration also takes into account the fact that by implementing EU law, provisions resulting from the GDPR and related national laws, are subject to the Charter of Fundamental Rights of the Union<sup>20</sup>. However, this does not impose additional obligations on controllers outside the Union in respect of processing not falling under the territorial scope of the GDPR.

## 2 APPLICATION OF THE TARGETING CRITERION – ART 3(2)

The absence of an establishment in the Union does not necessarily mean that processing activities by a data controller or processor established in a third country will be excluded from the scope of the GDPR, since Article 3(2) sets out the circumstances in which the GDPR applies to a controller or processor not established in the Union, depending on their processing activities.

In this context, the EDPB confirms that in the absence of an establishment in the Union, a controller or processor cannot benefit from the one-stop shop mechanism provided for in Article 56 of the GDPR. Indeed, the GDPR's cooperation and consistency mechanism only applies to controllers and processors with an establishment, or establishments, within the European Union<sup>21</sup>.

While the present guidelines aim to clarify the territorial scope of the GDPR, the EDPB also wish to stress that controllers and processors will also need to take into account other applicable texts, such as for instance EU or Member States' sectorial legislation and national laws. Several provisions of the GDPR indeed allow Member States to introduce additional conditions and to define a specific data protection framework at national level in certain areas or in relation to specific processing situations.

---

<sup>19</sup> G29 WP169 - Opinion 1/2010 on the concepts of "controller" and "processor", adopted on 16<sup>th</sup> February 2010 and under revision by the EDPB.

<sup>20</sup> Charter of Fundamental Right of the European Union, 2012/C 326/02.

<sup>21</sup> G29 WP244 rev.1, 13th December 2016, Guidelines for identifying a controller or processor's lead supervisory authority - endorsed by the EDPB.

Controllers and processors must therefore ensure that they are aware of, and comply with, these additional conditions and frameworks which may vary from one Member State to the other. Such variations in the data protection provisions applicable in each Member State are particularly notable in relation to the provisions of Article 8 (providing that the age at which children may give valid consent in relation to the processing of their data by information society services may vary between 13 and 16), of Article 9 (in relation to the processing of special categories of data), Article 23 (restrictions) or concerning the provisions contained in Chapter IX of the GDPR (freedom of expression and information; public access to official documents; national identification number; employment context; processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; secrecy; churches and religious associations).

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 application of the “targeting criterion” towards data subjects who are in the Union, as per Article 3(2), can be triggered by processing activities carried out by a controller or processor not established in the Union which relate to two distinct and alternative types of activities provided that these processing activities relate to data subjects that are in the Union.. In addition to being applicable only to processing by a controller or processor not established in the Union, the targeting criterion largely focuses on what the “processing activities” are “related to”, which is to be considered on a case-by-case basis.

The EDPB stresses that a controller or processor may be subject to the GDPR in relation to some of its processing activities but not subject to the GDPR in relation to other processing activities. The determining element to the territorial application of the GDPR as per Article 3(2) lies in the consideration of the processing activities in question.

In assessing the conditions for the application of the targeting criterion, the EDPB therefore recommends a twofold approach, in order to determine first that the processing relates to personal data of data subjects who are in the Union, and second whether processing relates to the offering of goods or services or to the monitoring of data subjects’ behaviour in the Union.

### a) Data subjects in the Union

The wording of Article 3(2) refers to “*personal data of data subjects who are in the Union*”. The application of the targeting criterion is therefore not limited by the citizenship, residence or other type of legal status of the data subject whose personal data are being processed. Recital 14 confirms this interpretation and states that “[t]he protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data”.

This provision of the GDPR reflects EU primary law which also lays down a broad scope for the protection of personal data, not limited to EU citizens, with Article 8 of the Charter of Fundamental Rights providing that the right to the protection of personal data is not limited but is for “everyone”<sup>22</sup>.

---

<sup>22</sup> Charter of Fundamental Right of the European Union, Article 8(1), « Everyone has the right to the protection of personal data concerning him or her ».

While the location of the data subject in the territory of the Union is a determining factor for the application of the targeting criterion as per Article 3(2), the EDPB considers that the nationality or legal status of a data subject who is in the Union cannot limit or restrict the territorial scope of the Regulation.

The requirement that the data subject be located in the Union must be assessed at the moment when the relevant trigger activity takes place, i.e. at the moment of offering of goods or services or the moment when the behaviour is being monitored, regardless of the duration of the offer made or monitoring undertaken.

The EDPB considers however that, in relation to processing activities related to the offer of services, the provision is aimed at activities that intentionally, rather than inadvertently or incidentally, target individuals in the EU. Consequently, if the processing relates to a service that is only offered to individuals outside the EU but the service is not withdrawn when such individuals enter the EU, the related processing will not be subject to the GDPR. In this case the processing is not related to the intentional targeting of individuals in the EU but relates to the targeting of individuals outside the EU which will continue whether they remain outside the EU or whether they visit the Union.

**Example 8:** An Australian company offers a mobile news and video content service, based on users' preferences and interest. Users can receive daily or weekly updates. The service is offered exclusively to users located in Australia, who must provide an Australian phone number when subscribing.

An Australian subscriber of the service travels to Germany on holiday and continues using the service.

Although the Australian subscriber will be using the service while in the EU, the service is not 'targeting' individuals in the Union, but targets only individuals in Australia, and so the processing of personal data by the Australian company does not fall within the scope of the GDPR.

**Example 9:** A start-up established in the USA, without any business presence or establishment in the EU, provides a city-mapping application for tourists. The application processes personal data concerning the location of customers using the app (the data subjects) once they start using the application in the city they visit, in order to offer targeted advertisement for places to visits, restaurant, bars and hotels. The application is available for tourists while they visit New York, San Francisco, Toronto, Paris and Rome.

The US start-up, via its city mapping application, is specifically targeting individuals in the Union (namely in Paris and Rome) through offering its services to them when they are in the Union. The processing of the EU-located data subjects' personal data in connection with the offering of the service falls within the scope of the GDPR as per Article 3(2)a. Furthermore, by processing data subject's location data in order to offer targeted advertisement on the basis of their location, the processing activities also relate to the monitoring of behaviour of individuals in the Union. The US start-up processing therefore also falls within the scope of the GDPR as per Article 3(2)b.

The EDPB also wishes to underline that the fact of processing personal data of an individual in the Union alone is not sufficient to trigger the application of the GDPR to processing activities of a controller or processor not established in the Union. The element of "targeting" individuals in the EU, either by offering goods or services to them or by monitoring their behaviour (as further clarified below), must always be present in addition.

**Example 10:** A U.S. citizen is travelling through Europe during his holidays. While in Europe, he downloads and uses a news app that is offered by a U.S. company. The app is exclusively directed at the U.S. market, evident by the app terms of use and the indication of US Dollar as the sole currency available for payment. The collection of the U.S. tourist's personal data via the app by the U.S. company is not subject to the GDPR.

Moreover, it should be noted that the processing of personal data of EU citizens or residents that takes place in a third country does not trigger the application of the GDPR, as long as the processing is not related to a specific offer directed at individuals in the EU or to a monitoring of their behaviour in the Union.

**Example 11:** A bank in Taiwan has customers that are residing in Taiwan but hold German citizenship. The bank is active only in Taiwan; its activities are not directed at the EU market. The bank's processing of the personal data of its German customers is not subject to the GDPR.

**Example 12:** The Canadian immigration authority processes personal data of EU citizens when entering the Canadian territory for the purpose of examining their visa application. This processing is not subject to the GDPR.

b) Offering of goods or services, irrespective of whether a payment by the data subject is required, to data subjects in the Union

The first activity triggering the application of Article 3(2) is the “offering of goods or services”, a concept which has been further addressed by EU law and case law, which should be taken into account when applying the targeting criterion. The offering of services also includes the offering of information society services, defined in point (b) of Article 1(1) of Directive (EU) 2015/1535<sup>23</sup> as “*any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services*”.

Article 3(2)(a) specifies that the targeting criterion concerning the offering of goods or services applies irrespective of whether a payment by the data subject is required. Whether the activity of a controller or processor not established in the Union is to be considered as an offer of a good or a service is not therefore dependent whether payment is made in exchange for the goods or services provided<sup>24</sup>.

**Example 13:** A US company, without any establishment in the EU, processes personal data of its employees that were on a temporary business trip to France, Belgium and the Netherlands for human resources purposes, in particular to proceed with the reimbursement of their accommodation expenses and the payment of their daily allowance, which vary depending on the country they are in.

In this situation, while the processing activity is specifically connected to persons on the territory of the Union (i.e. employees who are temporarily in France, Belgium and the Netherlands) it does not relate to an offer of a service to those individuals, but rather is part of the processing necessary for the employer to fulfil its contractual obligation and human resources duties related to the individual's

<sup>23</sup> Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services.

<sup>24</sup> See, in particular, CJEU, C-352/85, Bond van Adverteerders and Others vs. The Netherlands State, 26 April 1988, par. 16), and CJEU, C-109/92, Wirth [1993] Racc. I-6447, par. 15.

employment. The processing activity does not relate to an offer of service and is therefore not subject to the provision of the GDPR as per Article 3(2)a.

Another key element to be assessed in determining whether the Article 3(2)(a) targeting criterion can be met is whether the offer of goods or services is directed at a person in the Union, or in other words, whether the conduct on the part of the controller, which determines the means and purposes of processing, demonstrates its intention to offer goods or services to a data subject located in the Union. Recital 23 of the GDPR indeed clarifies that *“in order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union.”*

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

The elements listed in Recital 23 echo and are in line with the CJEU case law based on Council Regulation 44/2001<sup>25</sup> on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, and in particular its Article 15(1)(c). In *Pammer v Reederei Karl Schlüter GmbH & Co and Hotel Alpenhof v Heller* (Joined cases C-585/08 and C-144/09), the Court was asked to clarify what it means to “direct activity” within the meaning of Article 15(1)(c) of Regulation 44/2001 (*Brussels I*). The CJEU held that, in order to determine whether a trader can be considered to be “directing” its activity to the Member State of the consumer’s domicile, within the meaning of Article 15(1)(c) of Brussels I, the trader must have manifested its intention to establish commercial relations with such consumers. In this context, the CJEU considered evidence able to demonstrate that the trader was envisaging doing business with consumers domiciled in a Member State.

While the notion of “directing an activity” differs from the “offering of goods or services”, the EDPB deems this case law in *Pammer v Reederei Karl Schlüter GmbH & Co and Hotel Alpenhof v Heller* (Joined cases C-585/08 and C-144/09)<sup>26</sup> might be of assistance when considering whether goods or services are offered to a data subject in the Union. When taking into account the specific facts of the case, the following factors could therefore *inter alia* be taken into consideration, possibly in combination with one another:

- The EU or at least one Member State is designated by name with reference to the good or service offered;
- The data controller or processor pays a search engine operator for an internet referencing service in order to facilitate access to its site by consumers in the Union; or the controller or processor has launched marketing and advertisement campaigns directed at an EU country audience
- The international nature of the activity at issue, such as certain tourist activities;

---

<sup>25</sup> Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

<sup>26</sup> It is all the more relevant that, under Article 6 of 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), in absence of choice of law, this criterion of “directing activity” to the country of the consumer’s habitual residence is taken into account to designate the law of the consumer’s habitual residence as the law applicable to the contract.

- The mention of dedicated addresses or phone numbers to be reached from an EU country;
- The use of a top-level domain name other than that of the third country in which the controller or processor is established, for example “.de”, or the use of neutral top-level domain names such as “.eu”;
- The description of travel instructions from one or more other EU Member States to the place where the service is provided;
- The mention of an international clientele composed of customers domiciled in various EU Member States, in particular by presentation of accounts written by such customers;
- The use of a language or a currency other than that generally used in the trader’s country, especially a language or currency of one or more EU Member states;
- The data controller offers the delivery of goods in EU Member States.

As already mentioned, several of the elements listed above, if taken alone may not amount to a clear indication of the intention of a data controller to offer goods or services to data subjects in the Union, however, they should each be taken into account in any *in concreto* analysis in order to determine whether the combination of factors relating to the data controller’s commercial activities can together be considered as an offer of goods or services directed at data subjects in the Union.

It is however important to recall that Recital 23 confirms that the mere accessibility of the controller’s, processor’s or an intermediary’s website in the Union, the mention on the website of its e-mail or geographical address, or of its telephone number without an international code, does not, of itself, provide sufficient evidence to demonstrate the controller or processor’s intention to offer goods or a services to a data subject located in the Union. In this context, the EDPB recalls that when goods or services are inadvertently or incidentally provided to a person on the territory of the Union, the related processing of personal data would not fall within the territorial scope of the GDPR.

**Example 14:** A website, based and managed in Turkey, offers services for the creation, editing, printing and shipping of personalised family photo albums. The website is available in English, French, Dutch and German and payments can be made in Euros. The website indicates that photo albums can only be delivered by post mail in France, Benelux countries and Germany.

In this case, it is clear that the creation, editing and printing of personalised family photo albums constitute a service within the meaning of EU law. The fact that the website is available in four languages of the EU and that photo albums can be delivered by post in six EU Member States demonstrates that there is an intention on the part of the Turkish website to offer its services to individuals in the Union.

As a consequence, it is clear that the processing carried out by the Turkish website, as a data controller, relates to the offering of a service to data subjects in the Union and is therefore subject to the obligations and provisions of the GDPR, as per its Article 3(2)(a).

In accordance with Article 27, the data controller will have to designate a representative in the Union.

**Example 15:** A private company based in Monaco processes personal data of its employees for the purposes of salary payment. A large number of the company’s employees are French and Italian residents.

In this case, while the processing carried out by the company relates to data subjects in France and Italy, it does not takes place in the context of an offer of goods or services. Indeed human resources management, including salary payment by a third-country company cannot be considered as an offer of service within the meaning of Art 3(2)a. The processing at stake does not relate to the offer of goods

or services to data subjects in the Union (nor to the monitoring of behaviour) and, as a consequence, is not subject to the provisions of the GDPR, as per Article 3.

This assessment is without prejudice to the applicable law of the third country concerned.

**Example 16:** A Swiss University in Zurich is launching its Master degree selection process, by making available an online platform where candidates can upload their CV and cover letter, together with their contact details. The selection process is open to any student with a sufficient level of German and English and holding a Bachelor degree. The University does not specifically advertise to students in EU Universities, and only takes payment in Swiss currency.

As there is no distinction or specification for students from the Union in the application and selection process for this Master degree, it cannot be established that the Swiss University has the intention to target students from a particular EU member states. The sufficient level of German and English is a general requirement that applies to any applicant whether a Swiss resident, a person in the Union or a student from a third country. Without other factors to indicate the specific targeting of students in EU member states, it therefore cannot be established that the processing in question relates to the offer of an education service to data subject in the Union, and such processing will therefore not be subject to the GDPR provisions.

The Swiss University also offers summer courses in international relations and specifically advertises this offer in German and Austrian universities in order to maximise the courses' attendance. In this case, there is a clear intention from the Swiss University to offer such service to data subjects who are in the Union, and the GDPR will apply to the related processing activities.

### c) Monitoring of data subjects' behaviour

The second type of activity triggering the application of Article 3(2) is the monitoring of data subject behaviour as far as their behaviour takes place within the Union.

Recital 24 clarifies that “[t]he processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union.”

For Article 3(2)(b) to trigger the application of the GDPR, the behaviour monitored must first relate to a data subject in the Union and, as a cumulative criterion, the monitored behaviour must take place within the territory of the Union.

The nature of the processing activity which can be considered as behavioural monitoring is further specified in Recital 24 which states that “in order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.” While Recital 24 exclusively relates to the monitoring of a behaviour through the tracking of a person on the internet, the EDPB considers that tracking through other types of network or technology involving personal data processing should also be taken into account in determining whether a processing activity amounts to a behavioural monitoring, for example through wearable and other smart devices.

As opposed to the provision of Article 3(2)(a), neither Article 3(2)(b) nor Recital 24 expressly introduce a necessary degree of “intention to target” on the part of the data controller or processor to determine whether the monitoring activity would trigger the application of the GDPR to the processing activities. However, the use of the word “monitoring” implies that the controller has a specific purpose in mind for the collection and subsequent reuse of the relevant data about an individual’s behaviour within the EU. The EDPB does not consider that any online collection or analysis of personal data of individuals in the EU would automatically count as “monitoring”. It will be necessary to consider the controller’s purpose for processing the data and, in particular, any subsequent behavioural analysis or profiling techniques involving that data. The EDPB takes into account the wording of Recital 24, which indicates that to determine whether processing involves monitoring of a data subject behaviour, the tracking of natural persons on the Internet, including the potential subsequent use of profiling techniques, is a key consideration.

The application of Article 3(2)(b) where a data controller or processor monitors the behaviour of data subjects who are in the Union could therefore encompass a broad range of monitoring activities, including in particular:

- Behavioural advertisement
- Geo-localisation activities, in particular for marketing purposes
- Online tracking through the use of cookies or other tracking techniques such as fingerprinting
- Personalised diet and health analytics services online
- CCTV
- Market surveys and other behavioural studies based on individual profiles
- Monitoring or regular reporting on an individual’s health status

**Example 17:** A retail consultancy company established in the US provides advice on retail layout to a shopping centre in France, based on an analysis of customers’ movements throughout the centre collected through Wi-Fi tracking.

The analysis of a customers’ movements within the centre through Wi-Fi tracking will amount to the monitoring of individuals’ behaviour. In this case, the data subjects’ behaviour takes place in the Union since the shopping centre is located in France. The consultancy company, as a data controller, is therefore subject to the GDPR in respect of the processing of this data for this purpose as per its Article 3(2)(b).

In accordance with Article 27, the data controller will have to designate a representative in the Union.

**Example 18:** An app developer established in Canada with no establishment in the Union monitors the behaviour of data subject in the Union and is therefore subject to the GDPR, as per Article 3(2)b. The developer uses a processor established in the US for the app optimisation and maintenance purposes.

In relation to this processing, the Canadian controller has the duty to only use appropriate processors and to ensure that its obligations under the GDPR are reflected in the contract or legal act governing the relation with its processor in the US, pursuant to Article 28.

#### d) Processor not established in the Union

Processing activities which are “related” to the targeting activity which triggered the application of Article 3(2) fall within the territorial scope of the GDPR. The EDPB considers that there needs to be a

connection between the processing activity and the offering of good or service, but both processing by a controller and a processor are relevant and to be taken into account.

When it comes to a data processor not established in the Union, in order to determine whether its processing may be subject to the GDPR as per Article 3(2), it is necessary to look at whether the processing activities by the processor “are related” to the targeting activities of the controller.

The EDPB considers that, where processing activities by a controller relates to the offering of goods or services or to the monitoring of individuals’ behaviour in the Union (‘targeting’), any processor instructed to carry out that processing activity on behalf of the controller will fall within the scope of the GDPR by virtue of Art 3(2) in respect of that processing.

The ‘Targeting’ character of a processing activity is linked to its purposes and means; a decision to target individuals in the Union can only be made by an entity acting as a controller. Such interpretation does not rule out the possibility that the processor may actively take part in processing activities related to carrying out the targeting criteria (i.e. the processor offers goods or services or carries out monitoring actions on behalf of, and on instruction from, the controller).

The EDPB therefore considers that the focus should be on the connection between the processing activities carried out by the processor and the targeting activity undertaken by a data controller.

**Example 19:** A Brazilian company sells food ingredients and local recipes online, making this offer of good available to persons in the Union, by advertising these products and offering the delivery in the France, Spain and Portugal. In this context, the company instructs a data processor also established in Brazil to develop special offers to customers in France, Spain and Portugal on the basis of their previous orders and to carry out the related data processing.

Processing activities by the processor, under the instruction of the data controller, are related to the offer of good to data subject in the Union. Furthermore, by developing these customized offers, the data processor directly monitors data subjects in the EU. Processing by the processor are therefore subject to the GDPR, as per Article 3(2).

**Example 20:** A US company has developed a health and lifestyle app, allowing users to record with the US company their personal indicators (sleep time, weight, blood pressure, heartbeat, etc...). The app then provide users with daily advice on food and sport recommendations. The processing is carried out by the US data controller. The app is made available to, and is used by, individuals in the Union. For the purpose of data storage, the US company uses a processor established in the US (cloud service provider)

To the extent that the US company is monitoring the behaviour of individuals in the EU, in operating the health and lifestyle app it will be ‘targeting’ individuals in the EU and its processing of the personal data of individuals in the EU will fall within the scope of the GDPR under Art 3(2).

In carrying out the processing on instructions from, and on behalf of, the US company the cloud provider/processor is carrying out a processing activity ‘relating to’ the targeting of individuals in the EU by its controller. This processing activity by the processor on behalf of its controller falls within the scope of the GDPR under Art 3(2).

**Example 21:** A Turkish company offers cultural package travels in the Middle East with tour guides speaking English, French and Spanish. The package travels are notably advertised and offered through a website available in the three languages, allowing for online booking and payment in Euros and GBP. For marketing and commercial prospection purposes, the company instructs a data processor, a call

center, established in Tunisia to contact former customers in Ireland, France, Belgium and Spain in order to get feedback on their previous travels and inform them about new offers and destinations. The controller is ‘targeting’ by offering its services to individuals in the EU and its processing will fall within the scope of Art 3(2).

The processing activities of the Tunisian processor, which promotes the controllers’ services towards individuals in the EU, is also related to the offer of services by the controller and therefore falls within the scope of Art 3(2). Furthermore, in this specific case, the Tunisian processor actively takes part in processing activities related to carrying out the targeting criteria, by offering services on behalf of, and on instruction from, the Turkish controller.

#### e) Interaction with other GDPR provisions and other legislations

The EDPB will also further assess the interplay between the application of the territorial scope of the GDPR as per Article 3 and the provisions on international data transfers as per Chapter V. Additional guidance may be issued in this regard, should this be necessary.

Controllers or processors not established in the EU will be required to comply with their own third country national laws in relation to the processing of personal data. However, where such processing relates to the targeting of individuals in the Union as per Article 3(2) the controller will, in addition to being subject to its country’s national law, be required to comply with the GDPR. This would be the case regardless of whether the processing is carried out in compliance with a legal obligation in the third country or simply as a matter of choice by the controller.

### 3 PROCESSING IN A PLACE WHERE MEMBER STATE LAW APPLIES BY VIRTUE OF PUBLIC INTERNATIONAL LAW

Article 3(3) provides that “[t]his Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law”. This provision is expanded upon in Recital 25 which states that “[w]here Member State law applies by virtue of public international law, this Regulation should also apply to a controller not established in the Union, such as in a Member State’s diplomatic mission or consular post.”

The EDPB therefore considers that the GDPR applies to personal data processing carried out by EU Member States’ embassies and consulates located outside the EU as such processing falls within the scope of the GDPR by virtue of Article 3(3).. A Member State’s diplomatic or consular post, as a data controller or processor, would then be subject to all relevant provisions of the GDPR, including when it comes to the rights of the data subject, the general obligations related to controller and processor and the transfers of personal data to third countries or international organisations.

**Example 22:** The Dutch consulate in Kingston, Jamaica, opens an online application process for the recruitment of local staff in order to support its administration.

While the Dutch consulate in Kingston, Jamaica, is not established in the Union, the fact that it is a consular post of an EU country where Member State law applies by virtue of public international law renders the GDPR applicable to its processing of personal data, as per Article 3(3).

**Example 23:** A German cruise ship travelling in international waters is processing data of the guests on board for the purpose of tailoring the in-cruise entertainment offer.

While the ship is located outside the Union, in international waters, the fact that it is German-registered cruise ship means that by virtue of public international law the GDPR shall be applicable to its processing of personal data, as per Article 3(3).

Though not related to the application of Article 3(3), a different situation is the one where, by virtue of international law, certain entities, bodies or organisations established in the Union benefit from privileges and immunities such as those laid down in the Vienna Convention on Diplomatic Relations of 1961<sup>27</sup>, the Vienna Convention on Consular Relations of 1963 or headquarter agreements concluded between international organisations and their host countries in the Union. In this regard, the EDPB recalls that the application of the GDPR is without prejudice to the provisions of international law, such as the ones governing the privileges and immunities of non-EU diplomatic missions and consular posts, as well as international organisations. At the same time, it is important to recall that any controller or processor that falls within the scope of the GDPR for a given processing activity and that exchanges personal data with such entities, bodies and organisations have to comply with the GDPR, including where applicable its rules on transfers to third countries or international organisations.

## 4 REPRESENTATIVE OF CONTROLLERS OR PROCESSORS NOT ESTABLISHED IN THE UNION

Data controllers or processors subject to the GDPR as per its Article 3(2) are under the obligation to designate a representative in the Union. A controller or processor not established in the Union but subject to the GDPR failing to designate a representative in the Union would therefore be in breach of the Regulation.

This provision is not entirely new since Directive 95/46/EC already provided for a similar obligation. Under the Directive, this provision concerned controllers not established on Community territory that, for purposes of processing personal data, made use of equipment, automated or otherwise, situated on the territory of a Member State. The GDPR imposes an obligation to designate a representative in the Union to any controller or processor falling under the scope of Article 3(2), unless they meet the exemption criteria as per Article 27(2). In order to facilitate the application of this specific provision, the EDPB deems it necessary to provide further guidance on the designation process, establishment obligations and responsibilities of the representative in the Union as per Article 27.

It is worth noting that a controller or processor not established in the Union who has designated in writing a representative in the Union, in accordance with article 27 of the GDPR, does not fall within the scope of article 3(1), meaning that the presence of the representative within the Union does not constitute an “establishment” of a controller or processor by virtue of article 3(1).

### a) Designation of a representative

Recital 80 clarifies that “[t]he representative should be explicitly designated by a written mandate of the controller or of the processor to act on its behalf with regard to its obligations under this Regulation. The designation of such a representative does not affect the responsibility or liability of the controller or of the processor under this Regulation. Such a representative should perform its tasks according to

---

<sup>27</sup> [http://legal.un.org/ilc/texts/instruments/english/conventions/9\\_1\\_1961.pdf](http://legal.un.org/ilc/texts/instruments/english/conventions/9_1_1961.pdf)

*the mandate received from the controller or processor, including cooperating with the competent supervisory authorities with regard to any action taken to ensure compliance with this Regulation.”*

The written mandate referred to in Recital 80 shall therefore govern the relations and obligations between the representative in the Union and the data controller or processor established outside the Union, while not affecting the responsibility or liability of the controller or processor. The representative in the Union may be a natural or a legal person established in the Union able to represent a data controller or processor established outside the Union with regard to their respective obligations under the GDPR.

In practice, the function of representative in the Union can be exercised based on a service contract concluded with an individual or an organisation, and can therefore be assumed by a wide range of commercial and non-commercial entities, such as law firms, consultancies, private companies, etc... provided that such entities are established in the Union. One representative can also act on behalf of several non-EU controllers and processors.

When the function of representative is assumed by a company or any other type of organisation, it is recommended that a single individual be assigned as a lead contact and person “in charge” for each controller or processor represented. It would generally also be useful to specify these points in the service contract.

In line with the GDPR, the EDPB confirms that, when several processing activities of a controller or processor fall within the scope of Article 3(2) GDPR (and none of the exceptions of Article 27(2) GDPR apply), that controller or processor is not expected to designate several representatives for each separate processing activity falling within the scope of article 3(2). The EDPB does not consider the function of representative in the Union as compatible with the role of an external data protection officer (“DPO”) which would be established in the Union. Article 38(3) establishes some basic guarantees to help ensure that DPOs are able to perform their tasks with a sufficient degree of autonomy within their organisation. In particular, controllers or processors are required to ensure that the DPO “*does not receive any instructions regarding the exercise of [his or her] tasks*”. Recital 97 adds that DPOs, “*whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner*”<sup>28</sup>. Such requirement for a sufficient degree of autonomy and independence of a data protection officer does not appear to be compatible with the function of representative in the Union. The representative is indeed subject to a mandate by a controller or processor and will be acting on its behalf and therefore under its direct instruction<sup>29</sup>. The representative is mandated by the controller or processor it represents, and therefore acting on its behalf in exercising its task, and such a role cannot be compatible with the carrying out of duties and tasks of the data protection officer in an independent manner.

Furthermore, and to complement its interpretation, the EDPB recalls the position already taken by the WP29 stressing that “*a conflict of interests may also arise for example if an external DPO is asked to represent the controller or processor before the Courts in cases involving data protection issues*”<sup>30</sup>.

Similarly, given the possible conflict of obligation and interests in cases of enforcement proceedings, the EDPB does not consider the function of a data controller representative in the Union as compatible

---

<sup>28</sup> WP29 Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01 - endorsed by the EDPB.

<sup>29</sup> An external DPO also acting as representative in the Union could not for example be in a situation where he is instructed, as a representative, to communicate to a data subject a decision or measure taken by the controller or processor which he or she, as a DPO, had deemed uncompliant with the provisions of the GDPR and advised against.

<sup>30</sup> WP29 Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01 - endorsed by the EDPB.

with the role of data processor for that same data controller, in particular when it comes to compliance with their respective responsibilities and compliance.

While the GDPR does not impose any obligation on the data controller or the representative itself to notify the designation of the latter to a supervisory authority, the EDPB recalls that, in accordance with Articles 13(1)a and 14(1)a, as part of their information obligations, controllers shall provide data subjects information as to the identity of their representative in the Union. This information shall for example be included in the [privacy notice and] upfront information provided to data subjects at the moment of data collection. A controller not established in the Union but falling under Article 3(2) and failing to inform data subjects who are in the Union of the identity of its representative would be in breach of its transparency obligations as per the GDPR. Such information should furthermore be easily accessible to supervisory authorities in order to facilitate the establishment of a contact for cooperation needs.

**Example 24:** The website referred to in example 12, based and managed in Turkey, offers services for the creation, edition, printing and shipping of personalised family photo albums. The website is available in English, French, Dutch and German and payments can be made in Euros or Sterling. The website indicates that photo albums can only be delivered by post mail in the France, Benelux countries and Germany. This website being subject to the GDPR, as per its Article 3(2)(a), the data controller must designate a representative in the Union.

The representative must be established in one of the Member States where the service offered is available, in this case either in France, Belgium, Netherlands, Luxembourg or Germany. The name and contact details of the data controller and its representative in the Union must be part of the information made available online to data subjects once they start using the service by creating their photo album. It must also appear in the website general privacy notice.

### b) Exemptions from the designation obligation<sup>31</sup>

While the application of Article 3(2) triggers the obligation to designate a representative in the Union for controllers or processors established outside the Union, Article 27(2) foresees derogation from the mandatory designation of a representative in the Union, in two distinct cases:

- processing is “occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10”, and such processing “is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing”.

In line with positions taken previously by the Article 29 Working Party, the EPDB considers that a processing activity can only be considered as “occasional” if it is not carried out regularly, and occurs outside the regular course of business or activity of the controller or processor<sup>32</sup>.

Furthermore, while the GDPR does not define what constitutes large-scale processing, the WP29 has previously recommended in its guidelines WP243 on data protection officers (DPOs) that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale: the number of data subjects concerned - either as a specific number or as a

<sup>31</sup> Part of the criteria and interpretation laid down in G29 WP243 rev.1 (Data Protection Officer) - endorsed by the EDPB can be used as a basis for the exemptions to the designation obligation.

<sup>32</sup> WP29 position paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR.

proportion of the relevant population; the volume of data and/or the range of different data items being processed; the duration, or permanence, of the data processing activity; the geographical extent of the processing activity<sup>33</sup>.

Finally, the EDPB highlights that the exemption from the designation obligation as per Article 27 refers to processing “unlikely to result in a risk to the rights and freedoms of natural persons”<sup>34</sup>, thus not limiting the exemption to processing unlikely to result in a high risk to the rights and freedoms of data subjects. In line with Recital 75, when assessing the risk to the rights and freedom of data subjects, considerations should be given to both the likelihood and severity of the risk.

Or

- processing is carried out “by a public authority or body”.

The qualification as a “public authority or body” for an entity established outside the Union will need to be assessed by supervisory authorities *in concreto* and on a case by case basis<sup>35</sup>. The EDPB notes that, given the nature of their tasks and missions, cases where a public authority or body in a third country would be offering goods or services to data subject in the Union, or would monitor their behaviour taking place within the Union, are likely to be limited.

### c) Establishment in one of the Member States where the data subjects whose personal data are processed

Article 27(3) foresees that “the representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are”. In cases where a significant proportion of data subjects whose personal data are processed are located in one particular Member State, the EDPB recommends, as a good practice, that the representative is established in that same Member State. However, the representative must remain easily accessible for data subjects in Member States where it is not established and where the services or goods are being offered or where the behaviour is being monitored.

The EDPB confirms that the criterion for the establishment of the representative in the Union is the location of data subjects whose personal data are being processed. The place of processing, even by a processor established in another Member State, is here not a relevant factor for determining the location of the establishment of the representative.

**Example 25:** An Indian pharmaceutical company, with neither business presence nor establishment in the Union and subject to the GDPR as per Article 3(2), sponsors clinical trials carried out by investigators (hospitals) in Belgium, Luxembourg and the Netherlands. The majority of patients participating to the clinical trials are situated in Belgium.

The Indian pharmaceutical company, as a data controller, shall designate a representative in the Union established in one of the three Member States where patients, as data subjects, are participating in

<sup>33</sup> WP29 guidelines on data protection officers (DPOs), adopted on 13<sup>th</sup> December 2016, as last revised on 5<sup>th</sup> April 2017, WP 243 rev.01 - endorsed by the EDPB.

<sup>34</sup> Article 27(2)(a) GDPR.

<sup>35</sup> The GDPR does not define what constitutes a ‘public authority or body’. The EDPB considers that such a notion is to be determined under national law. Accordingly, public authorities and bodies include national, regional and local authorities, but the concept, under the applicable national laws, typically also includes a range of other bodies governed by public law.

the clinical trial (Belgium, Luxembourg or the Netherlands). Since most patients are Belgian residents, it is recommended that the representative is established in Belgium. Should this be the case, the representative in Belgium should however be easily accessible to data subjects and supervisory authorities in the Netherlands and Luxembourg.

In this specific case, the representative in the Union could be the legal representative of the sponsor in the Union, as per Article 74 of Regulation (EU) 536/2014 on clinical trials, provided that it does not act as a data processor on behalf of the clinical trial sponsor, that it is established in one of the three Member States, and that both functions are governed by and exercised in compliance with each legal framework.

#### d) Obligations and responsibilities of the representative

The representative in the Union acts on behalf of the controller or processor it represents with regard to the controller or processor's obligations under the GDPR. This implies notably the obligations relating to the exercise of data subject rights, and in this regard and as already stated, the identity and contact details of the representative must be provided to data subjects in accordance with articles 13 and 14. While not itself responsible for complying with data subject rights, the representative must facilitate the communication between data subjects and the controller or processor represented, in order to make the exercise of data subjects' rights effective.

As per Article 30, the controller or processor's representative shall in particular maintain a record of processing activities under the responsibility of the controller or processor. The EDPB considers that, while the maintenance of this record is an obligation imposed on both the controller or processor and the representative,, the controller or processor not established in the Union is responsible for the primary content and update of the record and must simultaneously provide its representative with all accurate and updated information so that the record can also be kept and made available by the representative at all time At the same time, it is the representative's own responsibility to be able to provide it in line with Article 27, e.g. when being addressed by a supervisory authority according to Art. 27(4).

As clarified by recital 80, the representative should also perform its tasks according to the mandate received from the controller or processor, including cooperating with the competent supervisory authorities with regard to any action taken to ensure compliance with this Regulation. In practice, this means that a supervisory authority would contact the representative in connection with any matter relating to the compliance obligations of a controller or processor established outside the Union, and the representative shall be able to facilitate any informational or procedural exchange between a requesting supervisory authority and a controller or processor established outside the Union.

With the help of a team if necessary, the representative in the Union must therefore be in a position to efficiently communicate with data subjects and cooperate with the supervisory authorities concerned. This means that this communication should in principle take place in the language or languages used by the supervisory authorities and the data subjects concerned or, should this result in a disproportionate effort, that other means and techniques shall be used by the representative in order to ensure the effectiveness of communication. The availability of a representative is therefore essential in order to ensure that data subjects and supervisory authorities will be able to establish contact easily with the non-EU controller or processor. In line with Recital 80 and Article 27(5), the designation of a representative in the Union does not affect the responsibility and liability of the controller or of the processor under the GDPR and shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves. The GDPR does not establish a

substitutive liability of the representative in place of the controller or processor it represents in the Union.

It should however be noted that the concept of the representative was introduced precisely with the aim of facilitating the liaison with and ensuring effective enforcement of the GDPR against controllers or processors that fall under Article 3(2) of the GDPR. 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 articles 30 and article 58(1) a of the GDPR

The EDPB furthermore highlights that article 50 of the GDPR notably aims at facilitating the enforcement of legislation in relation to third countries and international organisation, and that the development of further international cooperation mechanisms in this regard is currently being considered.

# Guidelines



## **Guidelines 04/2021 on Codes of Conduct as tools for transfers**

**Version 2.0**

**Adopted on 22 February 2022**

## Version history

Version 2.0	22 February 2022	Adoption of the Guidelines after public consultation
Version 1.0	7 July 2021	Adoption of the Guidelines for public consultation

## EXECUTIVE SUMMARY

The GDPR requires in its Article 46 that controllers/processors shall put in place appropriate safeguards for transfers of personal data to third countries or international organisations. To that end, the GDPR diversifies the appropriate safeguards that may be used by organisations under Article 46 for framing transfers to third countries by introducing amongst others, codes of conduct as a new transfer mechanism (articles 40-3 and 46-2-e). In this respect, as provided by Article 40-3, once approved by the competent supervisory authority and having been granted general validity within the Union by the Commission, a code of conduct may be adhered to and used by controllers or processors not subject to the GDPR located in third countries for the purpose of providing appropriate safeguards to data transferred to third countries. Such controllers and processors are required to make binding and enforceable commitments, via contractual or other legally binding instruments, to apply the appropriate safeguards provided by the code including with regard to the rights of data subjects as required by Article 40-3. The guidelines provide elements that should be addressed in such commitments.

It should also be noted that a code intended for transfers adhered to by a data importer in a third country can be relied on by controllers/processors subject to the GDPR (i.e. data exporters) for complying with their obligations in case of transfers to third countries in accordance with the GDPR without the need for such controllers/processors to adhere to such code themselves.

In terms of content of a code intended for transfers and for the purpose of providing appropriate safeguards in the meaning of Article 46, a code of conduct should address the essential principles, rights and obligations arising under the GDPR for controllers/processors but also the guarantees that are specific to the context of transfers (such as with respect to the issue of onward transfers, conflict of laws in the third country). In light of safeguards provided by existing transfer tools under Article 46 GDPR and to ensure consistency in the level of protection, as well as taking into account the CJEU Schrems II ruling<sup>1</sup>, the guidelines provide a check-list of the elements to be covered by a code of conduct intended for transfers.

A code of conduct may originally be drawn up only for the purpose of specifying the application of the GDPR in accordance with Article 40-2 (“GDPR code”) or also as a code intended for transfers in accordance with Article 40-3. As a consequence, depending on the original scope and content of the code, it may need to be amended in order to cover all of the above-mentioned elements if it is to be used as a tool for transfers.

These guidelines, which complement the EDPB Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, provide clarification as to the role of the different actors involved for the setting of a code to be used as a tool for transfers and the adoption process with flow charts.

---

<sup>1</sup> Judgment of the Court (Grand Chamber) of 16 July 2020; Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems.

## Table of contents

EXECUTIVE SUMMARY .....	3
1 AIM OF THE GUIDELINES.....	5
2 WHAT ARE CODES OF CONDUCT AS A TOOL FOR TRANSFERS? .....	5
3 WHAT SHOULD BE THE CONTENT OF A CODE OF CONDUCT AS A TOOL FOR TRANSFERS? .....	7
4 WHO ARE THE ACTORS INVOLVED FOR THE SETTING UP OF A CODE TO BE USED AS A TOOL FOR TRANSFERS AND WHAT IS THEIR ROLE?.....	9
4.1 Code owner.....	9
4.2 Monitoring body .....	9
4.3 SAs.....	10
4.4 EDPB .....	10
4.5 Commission .....	10
5 ADOPTION PROCESS OF A CODE OF CONDUCT FOR TRANSFERS.....	10
6 WHAT ARE THE GUARANTEES TO BE PROVIDED UNDER THE CODE? .....	11
6.1 Binding and enforceable commitments to be implemented.....	11
6.2 Check-list of elements to be included in a code of conduct intended for transfers .....	13
Annex 1 - ADOPTION OF CODE OF CONDUCT FOR TRANSFERS – FLOW CHART .....	15
a -Adoption of a transnational code intended for transfers .....	15
b- Amendments to a transnational code to be used as a code intended for transfers .....	15

# The European Data Protection Board

Having regard to Article 70 (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”),

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,<sup>2</sup>

Having regard to Article 12 and Article 22 of its Rules of Procedure,

## HAS ADOPTED THE FOLLOWING GUIDELINES

### 1 AIM OF THE GUIDELINES

1. The aim of these guidelines is to specify the application of Article 40-3 of the GDPR relating to codes of conduct as appropriate safeguards for transfers of personal data to third countries in accordance with Article 46-2-e) of the GDPR. They also aim to provide practical guidance including on the content of such codes of conduct, their adoption process and the actors involved as well as the requirements to be met and guarantees to be provided by a code of conduct for transfers.
2. These guidelines should further act as a clear reference for all SAs, the Board and assist the European Commission (hereinafter “Commission”) in evaluating codes in a consistent manner and to streamline the procedures involved in the assessment process. They should also provide greater transparency, ensuring that code owners who intend to seek approval for a code of conduct intended to be used as a tool for transfers (“code(s) intended for transfers” hereafter) are fully aware of the process and understand the formal requirements and the appropriate thresholds required for setting up such a code of conduct.
3. The present guidelines complement the EDPB Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 which establish the general framework for the adoption of codes of conduct (hereinafter “Guidelines 1/2019”). The considerations set out in Guidelines 1/2019 notably regarding the admissibility, submission and criteria for approval are thus also valid in the context of the preparation of codes intended for transfers.

### 2 WHAT ARE CODES OF CONDUCT AS A TOOL FOR TRANSFERS?

4. The GDPR requires in its Article 46 that controllers/processors shall put in place appropriate safeguards for transfers of personal data to third countries or international organisations.
5. To that end, the GDPR diversifies the appropriate safeguards that may be used by organisations under Article 46 for framing transfers to third countries by introducing amongst others, codes of conduct as

---

<sup>2</sup> References to “Member States” made throughout this document should be understood as references to “EEA Member States”.

a new transfer mechanism (Articles 40-3 and 46-2-e). In this respect, as provided by Article 40-3, once approved by the competent supervisory authority (hereafter “competent SA”) and having been granted general validity within the Union by the Commission, a code of conduct may also be adhered to and used by controllers or processors not subject to the GDPR located in third countries for the purpose of providing appropriate safeguards to data transferred to third countries. Such controllers and processors are required to make binding and enforceable commitments, via contractual or other legally binding instruments, to apply the appropriate safeguards provided by the code including with regard to the rights of data subjects as required by Article 40-3.

6. Codes of conduct may be prepared by associations or other bodies representing categories of controllers or processors (code owners) as specified by Article 40-2. As indicated in the Guidelines 1/2019, a non-exhaustive list of possible code owners would include: trade and representative associations, sectoral organisations, academic organisations and interest groups. According to the same Guidelines, codes intended for transfers could for instance be elaborated by bodies representing a sector (e.g. association/federation from banking and finance, insurance sector) but could also be drawn up for separate sectors which have a common processing activity sharing the same processing characteristics and needs (e.g. HR code drawn up by association/federation of HR professionals, or code on children’s data). Such codes would thus allow controllers, processors in third countries, receiving data under the code, to frame these transfers while better addressing the specific processing needs of their sector or common processing activities. As such, they could serve as a more adapted tool compared to other transfer mechanisms that are available under Article 46. Codes of conduct to be used as a tool for transfers will notably allow a given controller or processor in a third country to provide appropriate safeguards for multiple transfers to a third country that are specific to a sector or data processing activity. In addition, entities using the codes of conduct do not need to be within the same group to frame their transfers (as is the case for BCRs).
7. It should also be noted that a code intended for transfers adhered to by a data importer in a third country can be relied on by controllers/processors subject to the GDPR (i.e. data exporter) for complying with their obligations in case of transfers to third countries in accordance with the GDPR without the need for such controller/processors to adhere to such code themselves. Therefore, a code intended for transfers could frame transfers from controller/processors that do not adhere to that code of conduct to controller/processors in a third country having adhered to that code of conduct, provided that a commitment to comply with the obligations set forth by the code of conduct when processing the transferred data, including, in particular, with regard to the rights of data subjects, is included in a binding instrument. This means that the data importer in the third country has to adhere to the code intended for transfers whereas data exporters subject to the GDPR do not necessarily have to adhere to such code. Groups of companies transferring data from entities subject to the GDPR to those outside of the EEA may also use a code of conduct as a transfer tool where the entities outside the EEA have adhered to that code intended for transfers and have undertaken binding and enforceable commitments related to the transfer.

**Example n°1<sup>3</sup>:** Company XYZ is headquartered in Italy and has affiliates in Germany, the Netherlands, Spain and Belgium. For the purpose of managing the IT tools used by the group, Company XYZ uses the services of a cloud service provider based in a third country with no presence in the EU. Data processed as part of the use of IT tools involves transfers of data from Company XYZ and its affiliates

---

<sup>3</sup>The example is without prejudice to EDPB Recommendations 01/2020 on measures that supplement transfer tools.

to the cloud service provider, for the purpose of storage of data. As the cloud service provider in the third country has adhered to a code of conduct to be used as a tool for transfers relating to cloud services approved under Article 40-5, data flows from Company XYZ and its affiliates to the cloud service provider can be framed with the code of conduct to which the cloud service provider has adhered. In this case, the use of a code of conduct by the cloud service provider instead of other transfer tools such as BCRs appears more appropriate to the extent that a code of conduct does not require the controller/processor acting as importers to have a presence in the EEA while a presence in the EEA is required for a group of companies for using BCRs. The code of conduct also presents benefits for addressing multiple transfers of data with a single tool compared to (fully) contractual solutions such as SCCs.

8. A code intended for transfers could also frame transfers from controllers/processors subject to the GDPR to controllers/processors in the third country having adhered to the same code of conduct for transfers, provided in any case as explained above that a commitment to comply with the obligations of the code of conduct including with respect to the rights of data subjects, as they are enshrined in the GDPR, is included in a binding instrument.

**Example n°2:** An association representing categories of controllers/processors involved in the same type of research activities for the health sector and involving regular transfers of data to third country controllers/processors develop a code of conduct which is also intended to be used as a tool for transfers. Relevant controllers/processors in the EEA adhere to this code of conduct which is also being adhered to by third country controllers/processors. The transfers of data to third country controllers/processors as part of the research activities can be framed with this code of conduct.

9. To the extent that it is most likely that codes intended for transfers would be used by relevant entities for framing transfers from more than one Member State and considering that those codes of conduct should have general validity according to Article 40-9 GDPR, they would as such qualify as “transnational codes” as defined in the Guidelines 1/2019<sup>4</sup>.

### 3 WHAT SHOULD BE THE CONTENT OF A CODE OF CONDUCT AS A TOOL FOR TRANSFERS?

10. As set out above, a code of conduct intended for transfers is one of the tools that can be used by organisations performing particular data processing activities - e.g. within a specific sector or a common processing activity which share the same processing characteristics and needs - for providing appropriate safeguards for transfers of personal data to a third country in accordance with Article 46.
11. Also, the provisions of Article 40-3, which refer to the fact that codes intended for transfers may be adhered to by controllers/processors not subject to the GDPR under Article 3, suggest that codes intended for transfers are, in part, or as a whole, more specifically designed for third country controllers/processors. Therefore, according to the EDPB, the object of a code intended for transfers

<sup>4</sup> Transnational codes refer to a code which covers processing activities in more than one Member State. See Guidelines 1/2019, Appendix 1 – Distinction between national and transnational codes.

should be to set out also the rules that will need to be complied with by the third country controller/processor (the data importer) to ensure that personal data is adequately protected in line with the requirements of Chapter V GDPR when being processed by such third country controller/processor (i.e. data importer).

12. More specifically in terms of content, for the purpose of providing appropriate safeguards in the meaning of Article 46, the following elements need to be addressed:
  - Essential principles, rights and obligations arising under the GDPR for controllers/processors; and
  - Guarantees that are specific to the context of transfers (such as with respect to the issue of onward transfers, conflict of laws in the third country).
13. In this regard, it is worth noting that a code of conduct may originally be drawn up only for the purpose of specifying the application of the GDPR in accordance with Article 40-2 ("GDPR code") or also as a code intended for transfers in accordance with Article 40-3. As a consequence, depending on the original scope and content of the code, it may need to be amended in order to cover all of the above-mentioned elements if it is to be used as a tool for transfers.

**Example n°3:** Association ABC gathering organisations operating in the direct marketing sector at EU level has adopted a code of conduct which aims at specifying the application of the transparency principle and associated requirements under the GDPR as part of the processing activities for such sector. The Association wishes to use this code of conduct as a tool for framing transfers outside the EEA. To the extent that the code of conduct is focused on the transparency principle, it would need to be amended in order to cover additionally the appropriate safeguards that are required for international transfers of personal data, all essential principles and main requirements arising under the GDPR (other than transparency) as well as include guarantees that are specific to the context of transfers in order to obtain approval for such code as a code intended for transfers.

14. In any event, in line with the clarifications provided by the EDPB in its Guidelines 1/2019, all elements providing for appropriate safeguards as referred above will need to be set out in the code in a manner that facilitates their effective application and specifies how they apply in practice to the specific processing activity or sector<sup>5</sup>.
15. A check-list of the elements to be included in a code intended for transfers so that it can be considered as providing appropriate safeguards is further provided and explained under section 6 of the present guidelines.

---

<sup>5</sup> See Guidelines 1/2019, section 6.

## 4 WHO ARE THE ACTORS INVOLVED FOR THE SETTING UP OF A CODE TO BE USED AS A TOOL FOR TRANSFERS AND WHAT IS THEIR ROLE?

### 4.1 Code owner

16. The code owner is the entity, association/federation or other body that will prepare a code of conduct intended for transfers or amend an approved “GDPR code” for using it as a tool for transfers and submit it to the competent SA for approval<sup>6</sup>.

### 4.2 Monitoring body

17. As for any code of conduct, a monitoring body will need to be identified as part of a code intended for transfers and accredited by the competent SA in line with Article 41. More precisely, its role will be to monitor that third country controllers/processors having adhered to such code comply with the rules set out in the code<sup>7</sup>.
18. Considering that codes of conduct intended for transfers are also or more specifically aimed for third country controllers/processors, it has to be made sure that monitoring bodies are capable of effectively monitoring the code as specified in the Guidelines 1/2019. Monitoring bodies acting in the framework of codes for transfers could be located either only inside or also outside of the EEA provided that the concerned monitoring body has an establishment in the EEA. In this context, the monitoring body’s establishment in the EEA shall be the one where the headquarters of the monitoring body are, or the place where the final decisions concerning monitoring activities are taken and also requires that an EEA entity shall be able to control the monitoring body’s entities outside the EEA and demonstrate full accountability for all decisions and actions (including its liability for any breaches).
19. In addition, a monitoring body in the EEA may subcontract its activities to an external entity outside the EEA, acting on its behalf, provided that such entity maintains the same competence and expertise as required by the code of conduct as well as by the accreditation requirements, and that the EEA monitoring body is able to ensure effective control over the services provided by the contracting entity and retains the decision-making power about monitoring activities. In order to ensure compliance with this accreditation requirements when the monitoring body subcontracts parts of its tasks, the monitoring body shall establish a contract or any other legal act under European Union law binding on the subcontractor with regard to the monitoring body in such a way that all subcontracted tasks will meet the requirements of the GDPR. Recourse to subcontracting does not result in the delegation of responsibilities: in any case, the monitoring body remains responsible for monitoring compliance with the code of conduct to the supervisory authority. The monitoring body ensures that all subcontractors meet the requirements set out by this accreditation requirements document, notably as regards independence, absence of conflict of interest and expertise. The monitoring body includes a specific clause in the contract signed with subcontractors to ensure the confidentiality of personal data that may, where applicable, be disclosed to the subcontractor during the monitoring tasks and puts in place appropriate safeguards in case of transfer of such personal data to its subcontractors.

---

<sup>6</sup> For further details on the requirements relating to the code owner, please refer to the definition of code owner in section 2 and section 5.3 of Guidelines 1/2019.

<sup>7</sup> For further details on the need to set up a monitoring body under a code of conduct, please refer to sections 11 and 12 of Guidelines 1/2019.

#### 4.3 SAs

20. In accordance with Article 40-5, the role of the competent SA will be to approve the draft code of conduct intended for transfers or amendments to it for using it as a tool for transfers and to accredit the monitoring body identified as part of the code with respect to additional accreditation requirements relating to codes of conduct for transfers.

#### 4.4 EDPB

21. In accordance with Articles 40-7 and 64-1-b, the EDPB will be asked to provide an opinion on the draft decision of a SA aiming to approve a code intended for transfers or amendment to a code of conduct for using it also as a tool for transfers<sup>8</sup>.

#### 4.5 Commission

22. As provided by Article 40-9, the Commission may decide by adopting an implementing act that a code intended for transfers and approved by a SA has general validity within the Union. Only those codes having been granted general validity within the Union may be relied upon for framing transfers.

### 5 ADOPTION PROCESS OF A CODE OF CONDUCT FOR TRANSFERS

23. It results from Articles 40-5 and 40-9 that to be adopted, a code intended for transfers shall first be approved by a competent SA in the EEA and then recognized by the Commission as having general validity within the Union by way of implementing act.
24. As mentioned in section 2 above, to the extent that codes intended for transfers are most likely to be used by controllers/processors for framing transfers from more than one Member State, they would as such qualify as “transnational codes” and should follow the procedure for approval for transnational codes, including the need for an Opinion from the EDPB, as specified in section 8 and Annex 4 of the Guidelines 1/2019<sup>9</sup>. In practice different scenarios may arise when an association/federation or other body intends to adopt a code of conduct for transfers:

- A draft code is designed as a “GDPR code” as well as intended to be used as a tool for transfers by third country controller/processors. Such draft code would first need to be approved by the competent SA according to the procedure for transnational codes, including an Opinion from the Board, and then recognized by the Commission as having general validity within the Union in accordance with Article 40-9. After completion of these steps, controllers/processors in third country may adhere to the code and the code may be used for providing appropriate safeguards for transfers of data to third countries.
- A code of conduct is initially designed and approved as a “GDPR code”. Such code is further expanded in view of being also used as a tool for transfers by third country controller/processors. The amendment to the code relating to transfers will need to be submitted to the competent SA for approval which will follow the procedure for transnational codes involving an Opinion from the Board. The amended code will then need to be recognized

---

<sup>8</sup> See the EDPB Document on the procedure for the development of informal “Codes of Conduct sessions” [https://edpb.europa.eu/sites/default/files/files/file1/edpb\\_documentprocedurecodesconductsessions\\_en.pdf](https://edpb.europa.eu/sites/default/files/files/file1/edpb_documentprocedurecodesconductsessions_en.pdf).

<sup>9</sup> See Guidelines 1/2019, Appendix 1 – Distinction between national and transnational codes.

by the Commission as having general validity within the Union in accordance with Article 40-9 after which controllers/in third country may adhere to such code and use it for providing appropriate safeguards for transfers of personal data to third countries.

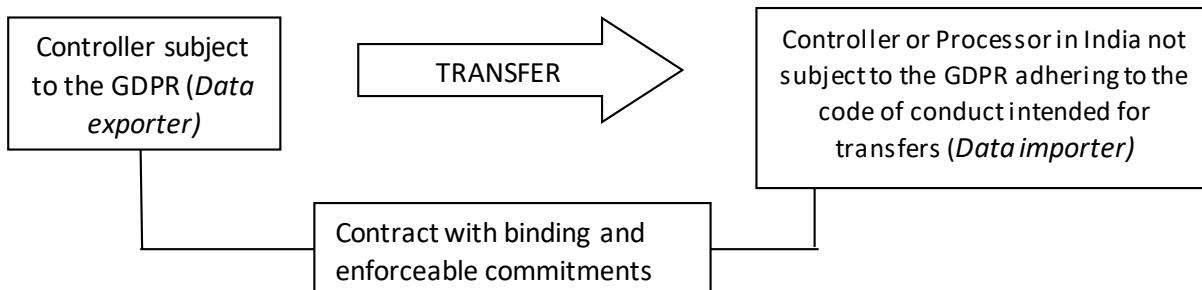
25. A flow chart set out in the annex to the guidelines details the procedural steps for adopting a code of conduct intended for transfer in consideration of the above possible scenarios.

## 6 WHAT ARE THE GUARANTEES TO BE PROVIDED UNDER THE CODE?

### 6.1 Binding and enforceable commitments to be implemented

26. The GDPR requires in its Article 40-3 that controllers and processors not subject to the GDPR adhering to a code intended for transfers take binding and enforceable commitments, via contractual or other legally binding instruments, to apply the appropriate safeguards provided by the code including, in particular, with regard to the rights of data subjects.
27. As specified by the GDPR, such commitments may be taken by using a contract, which appears as the most straightforward solution. Other instruments could also be used, provided that these controller/processors adhering to the code are able to demonstrate the binding and enforceable character of such other means.
28. In any event, the instrument needs to have a binding and enforceable nature in accordance with EU law and should also be binding and enforceable by data subjects as third-party beneficiaries.
29. A code of conduct as a transfer tool can have Code members located in the EEA, as well as Code members located outside the EEA. A distinction between Code members located in the EEA and Code members located outside the EEA is the direct application of the GDPR to the former but not the latter (provided that the latter does not fall under Article 3.2 GDPR).
30. As regards the Code members located outside the EEA, there is a need to ensure that their commitment to adhere to a “specified level of data protection” guarantees that the level of data protection provided for in the GDPR is not undermined. This is a prerequisite for their eligibility to participate in the code of conduct as a transfer tool.
31. To this end, a contract could be signed by the controller/processor in the third country (i.e. the data importer) with, for example, the entity transferring data under the code (i.e. data exporter). In practice, it could use an existing contract if any (e.g. service agreement between the exporter and the data importer or the contract to be put in place in accordance with Article 28 GDPR in case of importer-processors) in which the binding and enforceable commitments could be included. Another option could be to rely on a separate contract by adding to the code intended for transfers a model contract that would need to be then signed by, for instance, controllers/processors in the third country and all of its data exporters.
32. There should be flexibility to choose the most appropriate option depending on the specific situation.
33. When the code of conduct is to be used for transfers and onward transfers by a processor to sub-processors, a reference to the code of conduct and the instrument providing for binding and enforceable commitments should also be made in the processor agreement signed between the processor and its controller, where possible.

### Binding and enforceable commitments by the data importer (example)



34. In general, the contract or other instrument must set out that the controller/processor commits to comply with the rules specified in the code intended for transfers when processing data received under the code. The contract or other instrument shall also provide for mechanisms allowing to enforce such commitments in case of breaches by the controller/processor in particular with respect to the rights of data subjects whose data will be transferred under the code.
35. More particularly, the contract or other instrument should address:
  - The existence of a right for data subjects whose data are transferred under the code to enforce the rules under the code as third-party beneficiaries;
  - The issue of liability in case of breaches to the rules under the code by code member outside of the EEA. The code shall include a jurisdiction clause noting that data subjects shall have the possibility in case of violation of rules under the code by a code member outside the EEA to bring a claim, by invoking their third-party beneficiary right, including for compensation, against that entity before an EEA SAs and EEA court of the data subject's habitual residence. The code member outside the EEA shall accept the decision of the data subject to do so. Data subjects shall also have the possibility to bring any claim arising out or from the respect by the importer of the code of conduct against the data exporter before the SA or the court of the data exporter's establishment or of the data subject's habitual residence. This liability should be without prejudice to the mechanisms to be implemented under the code with the monitoring body that can also take action against controllers/processors in accordance with the code by imposing corrective measures. The data importer and the data exporter should also accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of the GDPR.
  - The existence of a right for the exporter to enforce against the code member acting as importer the rules under the code as a third-party beneficiary.
  - The existence of an obligation of the importer to notify the exporter and the Supervisory Authority of the data exporter of any detected violation of the code by the same code member acting as an importer outside the EEA and of any corrective measures taken by the monitoring body in response to that violation.

## 6.2 Check-list of elements to be included in a code of conduct intended for transfers

36. In light of safeguards provided by existing transfer tools under Article 46 GDPR (such as binding corporate rules), and to ensure consistency in the level of protection, as well as taking into account the CJEU Schrems II ruling<sup>10</sup>, the EDPB is of the view that to be considered as providing appropriate safeguards, the elements to be covered by a code of conduct intended for transfers should include the following:
- A description of transfers to be covered by the code (nature of data transferred, categories of data subjects, countries);
  - A description of the data protection principles to be complied with under the code (transparency, fairness and lawfulness, purpose limitation, data minimization and accuracy, limited storage of data, processing of sensitive data, security, for processors compliance with instructions from the controller), including rules on using processors or sub-processors and rules on onward transfers;
  - Accountability principle measures to be taken under the code;
  - The setting up of an appropriate governance through DPOs or other privacy staff in charge of compliance with data protection obligations resulting from the code;
  - The existence of a suitable training program on the obligations arising from the code;
  - The existence of a data protection audit (by either internal or external auditors) or other internal mechanism for monitoring compliance with the code, independently from the oversight to be performed by the monitoring body as for any code of conduct; Whereas the aim of the data protection audit program is to ensure and demonstrate compliance with the code, the aim of the audits performed by the monitoring body is to assess whether the applicant is eligible to participate to the code, continues to be eligible once it is a member, and whether sanctions are necessary in case of infringements;
  - Transparency measures, including easy access, regarding the use of the code in particular with respect to third party beneficiary rights;
  - The provision of data subject rights of access, rectification, erasure, restriction, notification regarding rectification or erasure or restriction, objection to processing, right not to be subject to decisions based solely on automated processing, including profiling as those provided for by Articles 12, 13, 14, 15, 16, 17, 18, 19, 21, and 22 GDPR;
  - The creation of third-party beneficiary rights for data subjects to enforce the rules of the code as third-party beneficiaries (as well as the possibility to lodge a complaint before the competent SA and before EEA Courts);
  - The existence of an appropriate complaint handling process for data protection rules infringements maintained by the monitoring body which if deemed appropriate may be complemented with an internal procedure to the code member for managing complaints;
  - A warranty that at the time of adhering to the code, the third country controller/processor has no reasons to believe that the laws applicable to the processing of personal data in the third country of transfer, prevent it from fulfilling its obligations under the code and to implement

---

<sup>10</sup> Judgment of the Court (Grand Chamber) of 16 July 2020; Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems.

where necessary together with the exporter supplementary measures<sup>11</sup> to ensure the required level of protection under EEA law<sup>12</sup>. In addition, a description of the steps to be taken (including notification to the exporter in the EEA, implementation of appropriate supplementary measures) in case after having adhered to the code the third country controller/processor becomes aware of any legislation of the third country preventing compliance by the code member with commitments taken as part of the code and measures to be taken in case of third country government access requests;

- The mechanisms for dealing with changes to the code;
  - The consequences of withdrawal of a member from the code;
  - A commitment for the code member and monitoring body to cooperate with EEA SAs;
  - A commitment for the code member to accept to be subject to the jurisdiction of EEA SAs in any procedure aimed at ensuring compliance with the code of conduct and EEA Courts;
  - The criteria of selection of the monitoring body for a code intended for transfers i.e. to demonstrate that the monitoring body has the requisite level of expertise to carry out its role in an effective manner for such a code intended for data transfers
37. In any event, it should be noted that these elements constitute minimum guarantees which may need to be complemented with additional commitments and measures depending on the transfer at stake under the code of conduct.
38. The EDPB will evaluate the functioning of these guidelines in light of the experience gained with their application in practice and provide further guidance to clarify the application of the above listed elements.

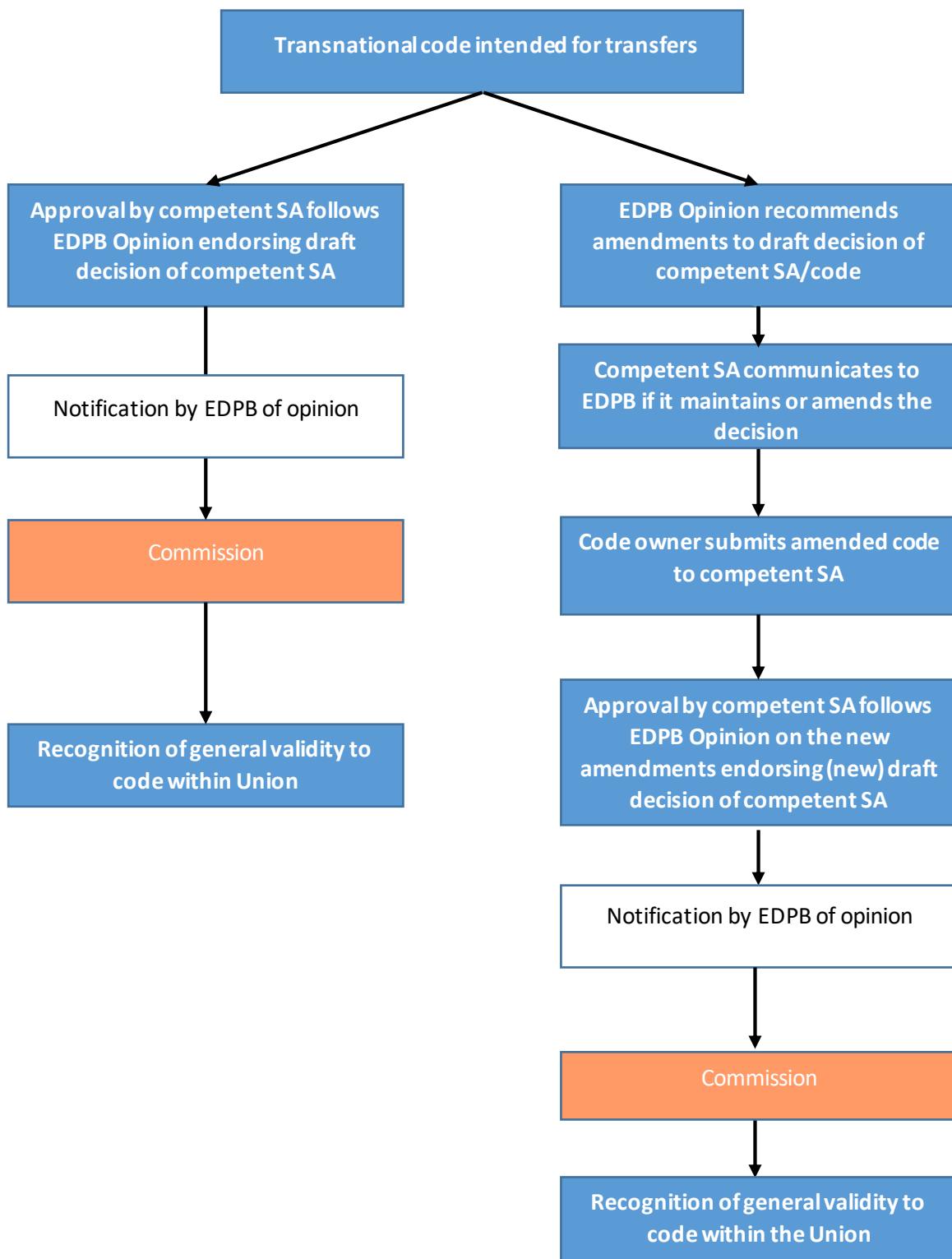
---

<sup>11</sup> The European Data Protection Board has published a Recommendation on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data which can assist in the assessment relating to the third country and for identifying appropriate supplementary measures.

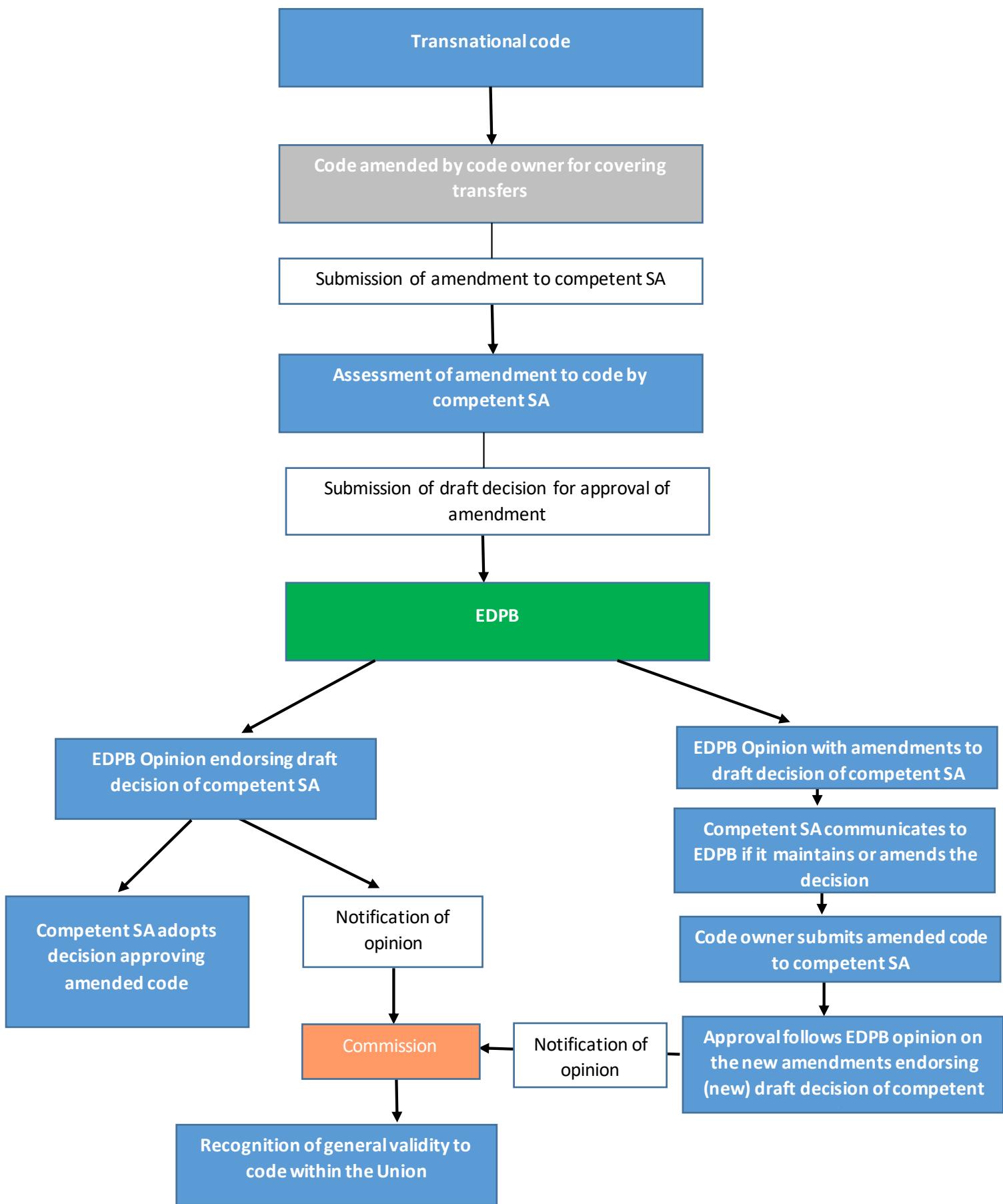
<sup>12</sup> This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with the safeguards specified in the code of conduct intended for transfers.

## ANNEX 1 - ADOPTION OF CODE OF CONDUCT FOR TRANSFERS – FLOW CHART

a -Adoption of a transnational code intended for transfers



b- Amendments to a transnational code to be used as a code intended for transfers



## Information Note

**on the redress mechanism for EU/EEA individuals in relation  
to alleged violations of U.S. law with respect to their data  
collected by U.S authorities competent for national security**

## **Context about complaints on government access by U.S. intelligence authorities**

On 10 July 2023, the European Commission adopted its Implementing Decision C(2023) 4745 on the adequate level of protection of personal data under the **EU-U.S. Data Privacy Framework ('DPF Adequacy decision')**<sup>1</sup>.

An important element of the U.S. legal framework, on which the adequacy decision is based, concerns **Executive Order 14086** on ‘Enhancing Safeguards for United States Signals Intelligence Activities’<sup>2</sup> (‘**E.O. 14086**’), which was signed by U.S. President Biden on 7 October 2022 and is accompanied by regulations adopted by the U.S. Attorney General, as well as relevant policies and procedures adopted by the U.S. Office of the Director of National Intelligence and U.S. Intelligence agencies.

E.O. 14086 established a **new redress mechanism in the area of national security** to handle and resolve complaints from data subjects in the EU and EEA,<sup>3</sup> alleging unlawful access and use of data by U.S. signals intelligence activities to their personal data that was transmitted from the EU and EEA to the U.S.<sup>4</sup> Thus, only complaints relating to national security will be considered under this redress mechanism. **This redress mechanism applies regardless of the transfer tool used to transfer the complainants' personal data to the U.S.** (i.e., DPF Adequacy decision, standard or ad hoc contractual clauses<sup>5</sup>, binding corporate rules<sup>6</sup>, codes of conduct<sup>7</sup>, certification mechanisms<sup>8</sup>, derogations<sup>9</sup>). However, this redress mechanism only applies to data transmitted **after 10 July 2023**.

*Please note that information about the possibility to complain about a private U.S. organization's compliance with the principles set out in the Data Privacy Framework can be found here: [https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-template-complaint-form\\_en](https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-template-complaint-form_en)*

## **How to lodge a complaint?**

Complaints have to be sent to the **national EU/EEA data protection authority** competent for the individual (**'DPA'**). A list of DPAs in the EU/EEA Member States can be found here: [https://edpb.europa.eu/about-edpb/about-edpb/members\\_en](https://edpb.europa.eu/about-edpb/about-edpb/members_en).

---

<sup>1</sup> Implementing Decision C(2023) 4745 of the European Commission, pursuant 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') on the adequate level of protection of personal data under the EU-US Data Privacy Framework ('the DPF Adequacy Decision') of 10 July 2023. By doing so, the Commission decided that the United States ('the U.S.'), for the purpose of Article 45 of the GDPR ensures an adequate level of protection for personal data transferred from the EU to organisations in the US that are included in the 'Data Privacy Framework List', maintained and made publicly available by the U.S. Department of Commerce (Article 1 of the Adequacy Decision), available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32023D1795>.

<sup>2</sup> Executive Order of October 7, 2022 on Enhancing Safeguards for United States Signals Intelligence Activities.

<sup>3</sup> References the “EU” made throughout this document should be understood as references to the “EEA”.

<sup>4</sup> Further specifications regarding this redress mechanism are also provided in the [E.O. 14086](#), as complemented by the [Attorney General Regulation on the Data Protection Review Court](#); see also Implementation Procedures for the Signals Intelligence Redress Mechanism Under Executive Order 14086 ('Intelligence Directive 126), available at: [https://www.dni.gov/files/documents/ICD/ICD\\_126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf](https://www.dni.gov/files/documents/ICD/ICD_126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf)

<sup>5</sup> Standard contractual clauses in accordance with Article 46(2)(c) or (d) GDPR, or ad hoc contractual clauses in accordance with Article 46(3)(a) GDPR.

<sup>6</sup> Article 46(2)(b) GDPR.

<sup>7</sup> Article 46(2)(e) GDPR.

<sup>8</sup> Article 46(2)(f) GDPR.

<sup>9</sup> Article 49 GDPR.

[The EDPB has adopted **Rules of Procedure** to provide guidance to DPAs in relation to their respective tasks and responsibilities.] An EU individual complaint form has been established for the submission of complaints to the CLPO by EU/EEA individuals

[https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/template-complaint-form-us-office-director-national\\_en](https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/template-complaint-form-us-office-director-national_en)

### **How will the DPA handle the complaint?**

The EU/EEA national DPA will **verify the identity of the individual complainants<sup>10</sup>** (for more information on how DPAs handle such verification, please also see: Link to each DPAs' procedure and will check that the complaint is complete and satisfies the conditions set forth in U.S. law<sup>11</sup>.

In particular that, the DPA will verify:

- The identity of the complainant, and that he/she is acting only on his/her own behalf and not as a representative of a governmental, non-governmental, or intergovernmental organisation;
- That the complainant believes that one or more U.S. law(s) have been violated if personal data of or about the complainant was unlawfully accessed by U.S. intelligence agencies after his/her personal data was transmitted from the EU to the U.S.;
- The complaint contains, in writing (also via email) all relevant information (**which need not demonstrate that the complainants' data has in fact been subject to US signals intelligence activities**):
  - any information that forms the basis of the complaint, including the details of the online account or personal data transfer believed to may have been accessed;
  - the nature of the relief sought<sup>12</sup>;
  - the specific means by which personal data of or about the complainants is believed to have been transmitted to the US;
  - which U.S. Government entity or entities believed to be involved in accessing the personal data of or about the complainant (if known);
  - and any other measures the complainant may have pursued to obtain the information or relief requested, and the response received through those other measures;
  - it pertains to personal data of or about the complainants, believed to have been transferred to the US after 10 July 2023;
- The complaint is not frivolous, vexatious or made in bad faith.

After this verification and if the complaint is found complete, the DPA will transmit it, in an encrypted format, to the **Secretariat of the European Data Protection Board ('EDPB**

---

<sup>10</sup> E.O. 14086, Section 4(k)(v) and Section E(1)(c)(8) of ICD 126.

<sup>11</sup> E.O 14086, Section 4(k)(i)-(iv).

<sup>12</sup> Such relief may include lawful measures designed to fully redress an identified violation. In a non-exhaustive manner, this may include administrative measures to remedy procedural or technical violations; deleting your personal data acquired without lawful authorization; deleting results of inappropriate queries on lawfully collected personal data; restricting access to your personal data.

**Secretariat’)<sup>13</sup>. The latter will then transmit it, in an encrypted format<sup>14</sup> to the U.S. authorities that are competent to handle the complaint, namely the Office of the Director of National Intelligence’s Civil Liberties Protection Officer (‘CLPO’).<sup>15</sup>**

### **What is the role of the CLPO?**

The CLPO is in charge of conducting an investigation of the complaint to determine whether the safeguards provided in E.O. 14086 or other applicable U.S. law(s) were violated and, if so, to determine the appropriate binding remediation<sup>16</sup>. The CLPO will provide a response<sup>17</sup> to the DPA, via the EDPB Secretariat, within a timely manner. This response will confirm that:

- (1) “The review either did not identify any covered violations or the Civil Liberties Protection officer of the Office of the Director of National Intelligence issued a determination requiring appropriate remediation”<sup>18</sup>. In its standardised response<sup>19</sup>, the ODNI CLPO will neither confirm nor deny whether the complainant has been the target of surveillance nor will it confirm the specific remedy that was applied;
- (2) The complainant or an element of the U.S. Intelligence Community may apply for review of the CLPO’s decision by submitting an appeal with the Data Protection Review Court (‘DPRC’); and
- (3) If either the complainant or an element of the Intelligence Community applies for review by the DPRC, a special advocate will be selected by the DPRC to advocate regarding the complainant’s interest in the matter (**‘Special Advocate’**).

The decision of the CLPO is binding on the elements of the Intelligence Community<sup>20</sup>.

The CLPO sends its response to the EDPB Secretariat in an encrypted format, which will then transmit it, also in an encrypted format, to the national DPA that originally received the complaint. This DPA will, in turn, inform the complainant of the CLPO’s response (including a translation from English, if and to the extent necessary).

### **How to appeal against the CLPO’s decision?**

Complainants have the possibility to appeal the decision of the CLPO before the **Data Protection Review Court (‘DPRC’) within 60 days** after receiving the notification by the national DPA of the CLPO’s response<sup>21</sup>. In order to appeal, the complainant may submit an application to **their DPA** within 60 days<sup>22</sup>. The DPRC can investigate complaints from

---

<sup>13</sup> Recital 177 of the Adequacy Decision.

<sup>14</sup> Section E(1)(f) of Intelligence Community Directive 126 states that: ‘If the CLPO determines that the complaint is not a qualifying complaint because it does not meet the conditions of Section E.1.c., or does not meet the conditions of Section E.1.d., of this Directive, the CLPO will provide written notification via **encrypted electronic communication and in the English language** to the appropriate public authority in a qualifying state of the deficiencies in the complaint.’

<sup>15</sup> For the purposes of this document, any references to the Civil Liberties Protection Officer (‘CLPO’) mean the Office of the Director of National Intelligence’s Civil Liberties Protection Officer (‘ODNI CLPO’).

<sup>16</sup> Section 3(c)(i)(E) and Section 3(d)(i)(H) of E.O. 14086.

<sup>17</sup> E.O. 14086, Section 3 (c)(i)E.

<sup>18</sup> E.O. 14086, Section 3 (c)(i)E(1).

<sup>19</sup> The standardised response will state that the CLPO’s “review either did not identify any covered violations or the Data Protection Review Court issued a determination requiring appropriate remediation” (E.O. 14086, Section 3 (c)(i)E).

<sup>20</sup> Section 3(c)(H)(ii) of E.O. 14086.

<sup>21</sup> The dates that will be taken into account to assess if the appeal was submitted within 60 days will be the date of notification to the complainant, by the DPA, of the CLPO’s determination, and the date of submission, by the complainant, of their appeal to the DPA.

<sup>22</sup> Recital 177 Adequacy Decision.

individuals in the EU/EEA, including obtaining relevant information from elements of the U.S. Intelligence Community, and can take binding remedial decisions<sup>23</sup>.

The appeal procedure will follow a similar channel and procedure as the initial complaint: The DPA will transmit the appeal to the EDPB Secretariat, in an encrypted format, which will in turn, transmit it, in an encrypted format, to the U.S. Department of Justice's Office of Privacy and Civil Liberties ('OPCL'), which provides support to the DPRC, so that the DPRC can review the appeal.

In particular, the DPRC will review the determinations made by the CLPO (both whether a violation of applicable U.S. law(s) occurred and as regards the appropriate remediation) based, at a minimum, on the record of the CLPO's investigation, as well as any information and submissions provided by the complainant, the Special Advocate or an element of the Intelligence Community<sup>24</sup>. A DPRC panel has access to all information necessary to conduct a review, which it may obtain through the CLPO (e.g. the panel may request the CLPO to supplement its record with additional information or factual findings if necessary to carry out the review)<sup>25</sup>. The Special Advocate also has access to all information necessary to fulfil their role of assisting the DPRC panel in its consideration of the application, including by advocating regarding the complainant's interest in the matter and by ensuring that the DPRC panel is well-informed of the issues and the law(s) with respect to the matter.

When concluding its review, the DPRC may:

- (1) decide that there is no evidence indicating that signals intelligence activities occurred involving personal data of the complainant;
- (2) decide that the CLPO's determinations were legally correct and supported by substantial evidence; or
- (3) if the DPRC disagrees with the determinations of the CLPO (whether a violation of applicable US law(s) occurred or the appropriate remediation), issue its own determinations<sup>26</sup>.

The decision of the DPRC is binding and final with respect to the complaint before it<sup>27</sup>. In cases where the DPRC's review was triggered by an application from the complainant<sup>28</sup>, the complainant is notified of the DPRC's decision. Once the DPRC completes its review, the DPRC will provide the complainant with a standardised statement indicating it has completed its review, and stating that "*the review either did not identify any covered violations or the Data Protection Review Court issued a determination requiring appropriate remediation.*"<sup>29</sup> The

---

<sup>23</sup> Section 3(c)(i)(E) and Section 3(d)(i)(H) of E.O. 14086.

<sup>24</sup> Recital 189 of the Adequacy Decision and Section 3(d)(i)(D) EO 14086.

<sup>25</sup> Recital 189 of Adequacy Decision; Section 3(d)(iii) EO 14086 and Section 201.9(b) AG Regulation.

<sup>26</sup> Recital 190 of Adequacy Decision and Section 3(d)(i)(E) EO 14086 and Section 201.9(c)-(e) AG Regulation. According to the definition of 'appropriate remediation', in Section 4(a) EO 14086, the DPRC must take into account "the ways that a violation of the kind identified have customarily been addressed" when deciding on a remedial measure to fully address a violation, i.e. the DPRC will consider, among other factors, how similar compliance issues were remedied in the past to ensure that the remedy is effective and appropriate.

<sup>27</sup> Recital 191 of Adequacy Decision and Section 3(d)(ii) EO 14086 and Section 201.9(g) AG Regulation.

<sup>28</sup> In accordance with Section 3(d)(i)(B) of EO 14086, elements of the Intelligence Community may also lodge applications for review of the determination made by the CLPO.

<sup>29</sup> Recital 192 Adequacy Decision and Section 3(d)(i)(H) EO 14086 and Section 201.9(h) AG Regulation. As regards the nature of the notification see Section 201.9 (h)(3) AG Regulation.

DPRC will transmit such statement, in an encrypted format, to the EDPB Secretariat, which will in turn transmit it to the DPA in an encrypted format. The DPA will notify the complainant of the DPRC's statement (including a translation from English, if and to the extent necessary). This statement will neither confirm nor deny whether the complainant has been the target of surveillance nor will it confirm the specific remedy that was applied. Each decision of the DPRC is also transmitted to the CLPO<sup>30</sup>.

### **What is the role of the U.S. Department of Commerce in relation to declassified information?**

The U.S. Department of Commerce ('DoC') will periodically contact the relevant elements of the Intelligence Community regarding whether information pertaining to the CLPO's or DPRC's review of a complaint has been declassified. If elements of the Intelligence Community inform the DoC that information pertaining to the CLPO's or DPRC's review of the complaint has been declassified, the DoC will notify the complainant, through the EDPB Secretariat, which will in turn transmit it to the DPA, that information pertaining to the review of their complaint by the CLPO or DPRC, as appropriate, may be available to the complainant under applicable US law<sup>31</sup>. One such law is the U.S. Freedom of Information Act ('FOIA')<sup>32</sup>, under which the complainant may submit a FOIA request directly to the ODNI, to the relevant Intelligence Community element, or to the Department of Justice (i.e., without going through the DPA and the EDPB Secretariat) for declassified information about their complaint. Instructions on how to submit FOIA requests are available on the respective public webpages<sup>33</sup>, the relevant Intelligence Community elements, and the DPRC<sup>34</sup>.

It should be noted that complaints from data subjects in the EU/EEA alleging certain violations of U.S. law(s) concerning U.S. signals intelligence activities adversely affecting their individual privacy and civil liberties and relating to their personal data that was transmitted from the EU/ EEA to the U.S. should only be submitted to the CLPO and not to the FOIA offices mentioned above.

---

<sup>30</sup> Recital 192 of Adequacy Decision and Section 201.9(h) AG Regulation.

<sup>31</sup> Section 3(d)(v)(C) of E.O. 14086.

<sup>32</sup> More information regarding the FOIA may be accessed at <https://www.dni.gov/index.php/foia>.

<sup>33</sup> <https://www.dni.gov/index.php/make-a-records-request>.

<sup>34</sup> <https://www.justice.gov/opcl/opcl-freedom-information-act>.

## Pre-GDPR BCRs overview list

The list of pre-GDPR BCRs provides information on BCRs which were submitted to supervisory authorities (SAs) for approval prior to 25 May 2018 and for which the informal cooperation procedure was closed successfully. The list states which SA took charge of coordinating the informal EU cooperation procedure.

Inclusion in the list does not imply endorsement by the EDPB of these BCRs. Inclusion in the list is without prejudice to any decision or measure the competent SA wishes to take, in particular regarding the BCRs or the processing involved.

Please note that this overview list is provided for information purposes only. Companies have a responsibility to inform the competent supervisory authorities of changes to the BCRs. The overview list is updated based on information provided by the company to the competent supervisory authorities.

Companies relying on BCRs for data transfers are obliged to give concerned data subjects easy access to their BCRs. For more details about the BCRs, please contact the company.

Title*	Type of BCR*	Closure of the EU cooperation	SA*	Terminated BCR	Updates	Last update of the overview*
ABN AMRO Group N.V.	Controller	2012	NL SA	N		20200703
Accenture	Controller	2009	UK SA		Lead SA change: IE SA as of March 2019	20200528
ADIENT	Controller		BE SA	N		20201021
AGCO	Controller		DE SA (Bavaria)	N		20201020
Air liquid	Controller	2018	FR SA			20201026
Airbus	Controller	2014	FR SA			20201026
Akastor ASA	Controller		NO SA			20180524
Aker Solutions ASA	Controller		NO SA			20180524
Akzo Nobel N.V.	Controller	2014	NL SA	N		20200706
Align Technologies, Inc.	Controller and Processor	2014	NL SA	N		20200706

\* Mandatory fields

Title*	Type of BCR*	Closure of the EU cooperation	SA*	Terminated BCR	Updates	Last update of the overview*
Allianz	Controller		DE SA (Bavaria)	N		20201020
American Express Company	Controller	2012	UK SA		BCR in effect as of 28 January 2013 Lead SA change: ES SA as of September 2019	20200528
AMGEN	Controller	2016	FR SA	N		20201026
Arcadis N.V.	Controller	2017	NL SA	N		20200706
ArcelorMittal Group	Controller	2013	LU SA	N		20201030
Ardian	Controller	2013	FR SA	N	Name change: group was called Axa Private Equity	20201026
Astra Zeneca AB	Controller	2014	UK SA	N	Lead change: SE SA as of October 2020	20201030
Atos	Controller and Processor	2014	FR SA			20201026
Automated Data Processing Inc. (ADP)	Controller and Processor	2018 Controller 2018 Processor	NL SA	N		20200703
AVAYA Group	Controller and Processor	2018	DE SA (Hessen)	Y		20201029
AXA	Controller	2013	FR SA	N		20201026
BakerCorp International Holdings Inc.	Controller	2015	NL SA			20200707
BMC Software	Controller and Processor	2015	FR SA			20201026
BMW	Controller		DE SA (Bavaria)	N		20201020
BNP Paribas SA	Controller	2018	FR SA			20201026

\* Mandatory fields

Title*	Type of BCR*	Closure of the EU cooperation	SA*	Terminated BCR	Updates	Last update of the overview*
Box, Inc	Controller and Processor	2016	UK SA			20200528
BP	Controller	2010	UK SA			20200528
Bristol Myers Squibb	Controller	2011	FR SA	N	Lead Authority change: IE SA as of June 2019 on date 20190625	20201026
BT Group Plc.	Controller and Processor	2017	UK SA		Lead Authority change: NL SA as of September 2020	20200901
CA Plc. (trading as CA Technologies)	Controller	2015	UK SA		Lead SA change: DE (Hessen) as of 28/08/2018	20200528
Capgemini	Controller and Processor	2016	FR SA			20201026
Cardinal Health, Inc	Controller		MT SA			20180524
CareFusion Inc.	Controller	2011	UK SA	Y	BCRs withdrawn 2019 at request of applicant	20200528
Cargill, Inc.	Controller	2013	UK SA		Lead change: NL SA as of July 2020	20200528
Christian Louboutin SAS	Controller	2018	FR SA			20201026
Cisco Systems, Inc.	Controller	2018	NL SA	N		20200706
Citigroup	Controller	2012	UK SA	N	BCR in effect as of 6 June 2013 Lead change: IE SA as of December 2020	20201020
CMA-CGM	Controller	2011	FR SA	N		20201026
Continental Group	Controller		DE SA (Lower Saxony)	N		20201021
Corning	Controller	2015	FR SA			20201026
Coöperatieve Rabobank U.A.	Controller	2014	NL SA	N		20200706
Danfoss A/S	Controller		DK SA			20201020

\* Mandatory fields

Title*	Type of BCR*	Closure of the EU cooperation	SA*	Terminated BCR	Updates	Last update of the overview*
Deutsche Post DHL	Controller	2011	DE SA (BFDI)	N		20201030
Deutsche Telekom	Controller	2014	DE SA (BFDI)	N		20201030
DNV GL	Controller		NO SA			20180524
DocuSign	Controller and Processor	2018	IE SA	N		20201020
DSM	Controller		NL SA			200117
e-Bay	Controller	2009	LU SA	N		20201030
ENGIE	Controller	2015	FR SA		Name change: group was called GDF SUEZ	20201026
EY	Controller and Processor	2013 Controller 2018 Processor	UK SA	N	Lead change: NL SA as of May 2019 Name change: group was called Ernst & Young	20200706
Festo Group	Controller	2017	DE SA (Baden-Württemberg)	N		20201118
First Data Corporation	Controller and Processor	2011	UK SA		Lead change: IE SA as of December 2020	20200528
Flex	Controller	2015	UK SA		Name change: group was called Flextronics International Ltd	20200528
Fluor Corporation INc.	Controller	2015	UK SA	N	Lead change: NL SA as of April 2020	20200703
General Electric (GE)	Controller and Processor	2012 Controller 2018 Processor	FR SA			20201026
Giesecke & Devrient	Controller and Processor		DE SA (Bavaria)	N		20201020
GlaxoSmithKline Plc	Controller	2013	UK SA		Lead change: IE SA as of October 2020	20200528

\* Mandatory fields

<b>Title*</b>	<b>Type of BCR*</b>	<b>Closure of the EU cooperation</b>	<b>SA*</b>	<b>Terminated BCR</b>	<b>Updates</b>	<b>Last update of the overview*</b>
Henner	Controller	2017	FR SA	Y	Company notified Lead SA of termination in March 2020	
Hermès	Controller	2012	FR SA	N		20201026
Hewlett Packard Company	Controller	2011	FR SA	Y	Corporate reorganisation: Hewlett Packard Company was split into 2 companies in 2015: HP Inc. and HP Enterprise	20201026
Hewlett Packard Enterprise	Controller and Processor	2011 Controller 2017 Processor	FR SA		Corporate reorganisation: Hewlett Packard Company was split into 2 companies in 2015: HP Inc. and HP Enterprise	20201026
Hewlett Packard Inc.	Controller and Processor	2011 Controller 2018 Processor	FR SA		Corporate reorganisation: Hewlett Packard Company was split into 2 companies in 2015: HP Inc. and HP Enterprise	20201026
Hyatt	Controller	2009	UK SA			20200528
IMS Health Incorporated	Controller	2010	UK SA	Y	BCRs withdrawn 2019 at request of applicant	20200528
ING Bank N.V.	Controller	2013	NL SA	N		20200706
Intel Corporation	Controller	2012	IE SA	N		20201020

\* Mandatory fields

<b>Title*</b>	<b>Type of BCR*</b>	<b>Closure of the EU cooperation</b>	<b>SA*</b>	<b>Terminated BCR</b>	<b>Updates</b>	<b>Last update of the overview*</b>
International Business Machines Corporation (IBM)	Controller	2017	UK SA		Lead change: NL SA as of September 2020	20200528
International SOS	Controller	2011	FR SA	N		20201026
ISS Group	Controller		DK SA			20201020
Itera ASA	Processor		NO SA			20180524
Jacobs Douwe Egberts N.V.	Controller	2011	NL SA	N	Name change: group was called D.E. Master Blenders 1753 ("DEMB") until 23 June 2015  Name change: group was called Sara Lee International B.V. (indirect subsidiary of Sara Lee Corporation) until 4 July 2011	20200706
John Deere	Controller	2018	DE SA (Baden-Württemberg)	N		20201118
Johnson Controls	Controller		BE SA	N		20201021
JPMC	Controller	2010	UK SA		Lead change: DE (Hessen) as of December 2020	20200528
Kongsberg	Controller		NO SA			20180524
Koninklijke DSM N.V.	Controller		NL SA			20200706
Koninklijke Vopak N.V.	Controller	2017	NL SA	N		20200706
Kvaerner ASA	Controller		NO SA			20180524
Latham & Watkins LLP	Controller	2016	UK SA		Lead change: DE (Hessen) as of December 2020	20200528

\* Mandatory fields

Title*	Type of BCR*	Closure of the EU cooperation	SA*	Terminated BCR	Updates	Last update of the overview*
LeasePlan Corporation N.V.	Controller	2015	NL SA	N		20200706
Ledvance	Controller		DE SA (Bavaria)	N		20201020
Lego Group	Controller		DK SA			20201020
Legrand	Controller	2014	FR SA			20201026
Linkbynet	Controller and Processor	2014	FR SA			20201026
Linklaters LLP	Controller	2012	UK SA		Lead SA change: BE SA as of 1 February 2020	20200528
Louis Vuitton Moët Hennessy (LVMH)	Controller	2010	FR SA	N		20201026
Maersk Group	Controller		DK SA			20201020
Marsh and McLennan Companies Inc.	Controller and Processor	2017	UK SA		Lead change: IE SA as of September 2020	20200528
Mastercard	Controller and Processor		BE SA	N		20201021
Merck Sharp & Dohme (MSD)	Controller		BE SA			20180524
Michelin	Controller	2010	FR SA	N		20201026
Microchip Technology Inc.	Controller	2009	UK SA		Name change: group was called the Atmel Corporation Lead SA change: NO SA as of October 2018	20200528
Motorola Mobility LLC	Controller	2013	UK SA			20200528
Motorola Solutions	Controller		UK SA	N	Lead Authority change: DK SA as of December 2020	20201020
NetApp, Inc.	Controller	2015	NL SA	N		20200706
NextiraOne Europe B.V.	Processor	2016	NL SA	N		20200706

\* Mandatory fields

Title*	Type of BCR*	Closure of the EU cooperation	SA*	Terminated BCR	Updates	Last update of the overview*
Norsk Hydro	Controller		NO SA			20180524
NOVARTIS	Controller	2012	FR SA	N		20201026
Novo Nordisk A/S	Controller		DK SA			20201020
Nutreco N.V.	Controller	2016	NL SA	N		20200706
Oracle EMEA Ltd	Processor	2017	IE SA	N		20201020
Osram	Controller		DE SA (Bavaria)	N		20201020
OVH	Controller	2012	FR SA	N		20201026
PayPal	Controller	2018	LU SA	N		20201030
Rakuten	Controller	2017	LU SA	N		20201030
Rockwool	Controller		DK SA			20201020
Royal Dutch Shell Plc.	Controller	2012	NL SA	N		20200706
Royal Philips Electronics	Controller and Processor	2012 Controller 2014 Processor	NL SA	N		20200706
Safran	Controller	2010	FR SA	N		20201026
Salesforce	Processor	2015	FR SA	N		20201026
Sanofi Aventis	Controller	2009	FR SA	N		20201026
Schlumberger Ltd.	Controller	2012	NL SA	N		20200706
Schneider Electric	Controller	2012	FR SA	N		20201026
Siemens Group	Controller		DE SA (Bavaria)	N		20201020
Simon-Kucher & Partners	Controller		DE SA (North Rhine-Westphalia)			20180524
Société Générale	Controller	2013	FR SA	N		20201026
Sopra HR Software	Controller and Processor	2012 Controller 2013 Processor	FR SA	N	Name change: group was called HR Access	20201026
Spencer Stuart	Controller	2011	UK SA			20200528
Starwoord Hotels and Resorts	Controller		BE SA	Y	As of 15 October 2018 the Starwood BCRs are terminated	20180524
Statoil ASA	Controller		NO SA			20180524
Telefonaktiebolaget LM Ericsson	Controller and Processor	2016 Processor	SE SA	N		20201030

\* Mandatory fields

Title*	Type of BCR*	Closure of the EU cooperation	SA*	Terminated BCR	Updates	Last update of the overview*
		2017 Controller				
Teleperformance <sup>2</sup>	Controller and Processor	2018	FR SA	N		20201026
TMF Group B.V.	Controller and Processor	2014	NL SA	N		20200706
TNT Express N.V.	Controller	2017	NL SA	N	Due to an acquisition of TNT by FedEx, the geographical scope of the BCR has been extended. The name of the group entity in the NL is "TNT Nederland B.V." and with the acquisition "Federal Express Corp. In the U.S. joined.	20200706
Total	Controller	2014	FR SA	N		20201026
Twilio Ireland Ltd	Controller and Processor	2018	IE SA	N		20201020
UCB	Controller		BE SA	N		20201021
United Technologies Corporation (UTC)	Controller		BE SA	N		20201021
Univar, Inc.	Controller	2017	NL SA	N		20200706
Verizon communications inc.	Controller and Processor	2018	UK SA		Lead change: IE SA as of December 2020	20200528
VMware International Limited	Processor	2018	IE SA	N		20201020
Workday	Processor	2018	IE SA	N		20201020
Yara	Controller		NO SA			20180524

\* Mandatory fields

<b>Title*</b>	<b>Type of BCR*</b>	<b>Closure of the EU cooperation</b>	<b>SA*</b>	<b>Terminated BCR</b>	<b>Updates</b>	<b>Last update of the overview*</b>
Zendesk International Limited	Controller and Processor	2017	IE SA	N		20201020

\* Mandatory fields

## Pre-GDPR BCRs overview list

The list of pre-GDPR BCRs provides information on BCRs which were submitted to supervisory authorities (SAs) for approval prior to 25 May 2018 and for which the informal cooperation procedure was closed successfully. The list states which SA took charge of coordinating the informal EU cooperation procedure.

Inclusion in the list does not imply endorsement by the EDPB of these BCRs. Inclusion in the list is without prejudice to any decision or measure the competent SA wishes to take, in particular regarding the BCRs or the processing involved.

Please note that this overview list is provided for information purposes only. Companies have a responsibility to inform the competent supervisory authorities of changes to the BCRs. The overview list is updated based on information provided by the company to the competent supervisory authorities.

Companies relying on BCRs for data transfers are obliged to give concerned data subjects easy access to their BCRs. For more details about the BCRs, please contact the company.

Title*	Type of BCR*	Closure of the EU cooperation	SA*	Terminated BCR	Updates	Last update of the overview*
ABN AMRO Group N.V.	Controller	2012	NL SA	N		20200703
Accenture	Controller	2009	UK SA		Lead SA change: IE SA as of March 2019	20200528
ADIENT	Controller		BE SA	N		20201021
AGCO	Controller		DE SA (Bavaria)	N		20201020
Air liquid	Controller	2018	FR SA			20201026
Airbus	Controller	2014	FR SA			20201026
Akastor ASA	Controller		NO SA			20180524
Aker Solutions ASA	Controller		NO SA			20180524
Akzo Nobel N.V.	Controller	2014	NL SA	N		20200706

\* Mandatory fields

Title*	Type of BCR*	Closure of the EU cooperation	SA*	Terminated BCR	Updates	Last update of the overview*
Align Technologies, Inc.	Controller and Processor	2014	NL SA	N		20200706
Allianz	Controller		DE SA (Bavaria)	N		20201020
American Express Company	Controller	2012	UK SA		BCR in effect as of 28 January 2013 Lead SA change: ES SA as of September 2019	20200528
AMGEN	Controller	2016	FR SA	N		20201026
Arcadis N.V.	Controller	2017	NL SA	N		20200706
ArcelorMittal Group	Controller	2013	LU SA	N		20201030
Ardian	Controller	2013	FR SA	N	Name change: group was called Axa Private Equity	20201026
Astra Zeneca AB	Controller	2014	UK SA	N	Lead change: SE SA as of October 2020	20201030
Atos	Controller and Processor	2014	FR SA			20201026
Automated Data Processing Inc. (ADP)	Controller and Processor	2018 Controller 2018 Processor	NL SA	N		20200703
AVAYA Group	Controller and Processor	2018	DE SA (Hessen)	N	Correction: BCR was mistakenly listed as terminated	20230303
AXA	Controller	2013	FR SA	N		20201026
BakerCorp International Holdings Inc.	Controller	2015	NL SA			20200707
BMC Software	Controller and Processor	2015	FR SA			20201026
BMW	Controller		DE SA (Bavaria)	N		20201020
BNP Paribas SA	Controller	2018	FR SA			20201026

\* Mandatory fields

Title*	Type of BCR*	Closure of the EU cooperation	SA*	Terminated BCR	Updates	Last update of the overview*
Box, Inc	Controller and Processor	2016	UK SA			20200528
BP	Controller	2010	UK SA			20200528
Bristol Myers Squibb	Controller	2011	FR SA	N	Lead Authority change: IE SA as of June 2019 on date 20190625	20201026
BT Group Plc.	Controller and Processor	2017	UK SA		Lead Authority change: NL SA as of September 2020	20200901
CA Plc. (trading as CA Technologies)	Controller	2015	UK SA		Lead SA change: DE (Hessen) as of 28/08/2018	20200528
Capgemini	Controller and Processor	2016	FR SA			20201026
Cardinal Health, Inc	Controller		MT SA			20180524
CareFusion Inc.	Controller	2011	UK SA	Y	BCRs withdrawn 2019 at request of applicant	20200528
Cargill, Inc.	Controller	2013	UK SA		Lead change: NL SA as of July 2020	20200528
Christian Louboutin SAS	Controller	2018	FR SA			20201026
Cisco Systems, Inc.	Controller	2018	NL SA	N		20200706
Citigroup	Controller	2012	UK SA	N	BCR in effect as of 6 June 2013 Lead change: IE SA as of December 2020	20201020
CMA-CGM	Controller	2011	FR SA	N		20201026
Continental Group	Controller		DE SA (Lower Saxony)	N		20201021
Corning	Controller	2015	FR SA			20201026
Coöperatieve Rabobank U.A.	Controller	2014	NL SA	N		20200706
Danfoss A/S	Controller		DK SA			20201020
Deutsche Post DHL	Controller	2011	DE SA (BFDI)	N		20201030
Deutsche Telekom	Controller	2014	DE SA (BFDI)	N		20201030
DNV GL	Controller		NO SA			20180524

\* Mandatory fields

Title*	Type of BCR*	Closure of the EU cooperation	SA*	Terminated BCR	Updates	Last update of the overview*
DocuSign	Controller and Processor	2018	IE SA	N		20201020
DSM	Controller		NL SA			200117
e-Bay	Controller	2009	LU SA	N		20201030
ENGIE	Controller	2015	FR SA		Name change: group was called GDF SUEZ	20201026
EY	Controller and Processor	2013 Controller 2018 Processor	UK SA	N	Lead change: NL SA as of May 2019 Name change: group was called Ernst & Young	20200706
Festo Group	Controller	2017	DE SA (Baden-Württemberg)	N		20201118
First Data Corporation	Controller and Processor	2011	UK SA		Lead change: IE SA as of December 2020	20200528
Flex	Controller	2015	UK SA		Name change: group was called Flextronics International Ltd	20200528
Fluor Corporation INc.	Controller	2015	UK SA	N	Lead change: NL SA as of April 2020	20200703
General Electric (GE)	Controller and Processor	2012 Controller 2018 Processor	FR SA			20201026
Giesecke + Devrient GmbH	Controller and Processor		DE SA (Bavaria)	N	Name change: group was called Giesecke&Devrient	20230317
GlaxoSmithKline Plc	Controller	2013	UK SA		Lead change: IE SA as of October 2020	20200528
Henner	Controller	2017	FR SA	Y	Company notified Lead SA of termination in March 2020	
Hermès	Controller	2012	FR SA	N		20201026
Hewlett Packard Company	Controller	2011	FR SA	Y	Corporate reorganisation: Hewlett Packard Company was split	20201026

\* Mandatory fields

Title*	Type of BCR*	Closure of the EU cooperation	SA*	Terminated BCR	Updates	Last update of the overview*
					into 2 companies in 2015: HP Inc. and HP Enterprise	
Hewlett Packard Enterprise	Controller and Processor	2011 Controller 2017 Processor	FR SA		Corporate reorganisation: Hewlett Packard Company was split into 2 companies in 2015: HP Inc. and HP Enterprise	20201026
Hewlett Packard Inc.	Controller and Processor	2011 Controller 2018 Processor	FR SA		Corporate reorganisation: Hewlett Packard Company was split into 2 companies in 2015: HP Inc. and HP Enterprise	20201026
Hyatt	Controller	2009	UK SA			20200528
IMS Health Incorporated	Controller	2010	UK SA	Y	BCRs withdrawn 2019 at request of applicant	20200528
ING Bank N.V.	Controller	2013	NL SA	N		20200706
Intel Corporation	Controller	2012	IE SA	N		20201020
International Business Machines Corporation (IBM)	Controller	2017	UK SA		Lead change: NL SA as of September 2020	20200528
International SOS	Controller	2011	FR SA	N		20201026
ISS Group	Controller		DK SA			20201020
Itera ASA	Processor		NO SA			20180524
Jacobs Douwe Egberts N.V.	Controller	2011	NL SA	N	Name change: group was called D.E. Master Blenders 1753 ("DEMB") until 23 June 2015  Name change: group was called Sara Lee International B.V. (indirect subsidiary of Sara	20200706

\* Mandatory fields

Title*	Type of BCR*	Closure of the EU cooperation	SA*	Terminated BCR	Updates	Last update of the overview*
					Lee Corporation) until 4 July 2011	
John Deere	Controller	2018	DE SA (Baden-Württemberg)	N		20201118
Johnson Controls	Controller		BE SA	N		20201021
JPMC	Controller	2010	UK SA		Lead change: DE (Hessen) as of December 2020	20200528
Kongsberg	Controller		NO SA			20180524
Koninklijke DSM N.V.	Controller		NL SA			20200706
Koninklijke Vopak N.V.	Controller	2017	NL SA	N		20200706
Kvaerner ASA	Controller		NO SA			20180524
Latham & Watkins LLP	Controller	2016	UK SA		Lead change: DE (Hessen) as of December 2020	20200528
LeasePlan Corporation N.V.	Controller	2015	NL SA	N		20200706
Ledvance	Controller		DE SA (Bavaria)	N		20201020
Lego Group	Controller		DK SA			20201020
Legrand	Controller	2014	FR SA			20201026
Linkbynet	Controller and Processor	2014	FR SA			20201026
Linklaters LLP	Controller	2012	UK SA		Lead SA change: BE SA as of 1 February 2020	20200528
Louis Vuitton Moët Hennessy (LVMH)	Controller	2010	FR SA	N		20201026
Maersk Group	Controller		DK SA			20201020
Marsh and McLennan Companies Inc.	Controller and Processor	2017	UK SA		Lead change: IE SA as of September 2020	20200528
Mastercard	Controller and Processor		BE SA	N		20201021
Merck Sharp & Dohme (MSD)	Controller		BE SA			20180524
Michelin	Controller	2010	FR SA	N		20201026

\* Mandatory fields

Title*	Type of BCR*	Closure of the EU cooperation	SA*	Terminated BCR	Updates	Last update of the overview*
Microchip Technology Inc.	Controller	2009	UK SA		Name change: group was called the Atmel Corporation Lead SA change: NO SA as of October 2018	20200528
Motorola Mobility LLC	Controller	2013	UK SA			20200528
Motorola Solutions	Controller		UK SA	N	Lead Authority change: DK SA as of December 2020	20201020
NetApp, Inc.	Controller	2015	NL SA	N		20200706
NextiraOne Europe B.V.	Processor	2016	NL SA	N		20200706
Norsk Hydro	Controller		NO SA			20180524
NOVARTIS	Controller	2012	FR SA	N		20201026
Novo Nordisk A/S	Controller		DK SA			20201020
Nutreco N.V.	Controller	2016	NL SA	N		20200706
Oracle EMEA Ltd	Processor	2017	IE SA	N		20201020
Osram	Controller		DE SA (Bavaria)	N		20201020
OVH	Controller	2012	FR SA	N		20201026
PayPal	Controller	2018	LU SA	N		20201030
Rakuten	Controller	2017	LU SA	N		20201030
Rockwool	Controller		DK SA			20201020
Royal Dutch Shell Plc.	Controller	2012	NL SA	N		20200706
Royal Philips Electronics	Controller and Processor	2012 Controller 2014 Processor	NL SA	N		20200706
Safran	Controller	2010	FR SA	N		20201026
Salesforce	Processor	2015	FR SA	N		20201026
Sanofi Aventis	Controller	2009	FR SA	N		20201026
Schlumberger Ltd.	Controller	2012	NL SA	N		20200706
Schneider Electric	Controller	2012	FR SA	N		20201026
Siemens Group	Controller		DE SA (Bavaria)	N		20201020

\* Mandatory fields

Title*	Type of BCR*	Closure of the EU cooperation	SA*	Terminated BCR	Updates	Last update of the overview*
Simon-Kucher & Partners	Controller		DE SA (North Rhine-Westphalia)			20180524
Société Générale	Controller	2013	FR SA	N		20201026
Sopra HR Software	Controller and Processor	2012 Controller 2013 Processor	FR SA	N	Name change: group was called HR Access	20201026
Spencer Stuart	Controller	2011	UK SA			20200528
Starwoord Hotels and Resorts	Controller		BE SA	Y	As of 15 October 2018 the Starwood BCRs are terminated	20180524
Statoil ASA	Controller		NO SA			20180524
Telefonaktiebolaget LM Ericsson	Controller and Processor	2016 Processor 2017 Controller	SE SA	N		20201030
Teleperformance <sup>2</sup>	Controller and Processor	2018	FR SA	N		20201026
TMF Group B.V.	Controller and Processor	2014	NL SA	N		20200706
TNT Express N.V.	Controller	2017	NL SA	N	Due to an acquisition of TNT by FedEx, the geographical scope of the BCR has been extended. The name of the group entity in the NL is "TNT Nederland B.V." and with the acquisition "Federal Express Corp. In the U.S. joined.	20200706
Total	Controller	2014	FR SA	N		20201026
Twilio Ireland Ltd	Controller and Processor	2018	IE SA	N		20201020
UCB	Controller		BE SA	N		20201021

\* Mandatory fields

Title*	Type of BCR*	Closure of the EU cooperation	SA*	Terminated BCR	Updates	Last update of the overview*
United Technologies Corporation (UTC)	Controller		BE SA	N		20201021
Univar Solutions	Controller	2017	NL SA	N	Name change: group was listed under 'Univar, Inc.'	20210114
Verizon communications inc.	Controller and Processor	2018	UK SA		Lead change: IE SA as of December 2020	20200528
VMware International Limited	Processor	2018	IE SA	N		20201020
Workday	Processor	2018	IE SA	N		20201020
Yara	Controller		NO SA			20180524
Zendesk International Limited	Controller and Processor	2017	IE SA	N		20201020

\* Mandatory fields

# Information note on data transfers under the GDPR to the United Kingdom after the transition period

## Adopted on 15 December 2020

The transition period for the United Kingdom's withdrawal from the European Union will end on 31 December 2020. This means that as of 1 January 2021, the UK will no longer apply the GDPR to the processing of personal data and a separate legal framework regarding data protection will be in force in the UK. Consequently, as of 1 January 2021, all transfers of personal data between stakeholders subject to GDPR and UK entities will constitute a transfer of personal data to a third country and therefore will be subject to the provisions of Chapter V GDPR.

In the absence of an adequacy decision applicable to the UK as per Article 45 GDPR, such transfers will require appropriate safeguards (e.g., standard data protection clauses, binding corporate rules<sup>1</sup>, codes of conduct...), as well as enforceable data subject rights and effective legal remedies for data subjects, in accordance with Article 46 GDPR.

Subject to specific conditions, it may still be possible to transfer personal data to the UK based on a derogation listed in Article 49 GDPR. However, Article 49 GDPR has an exceptional nature and the derogations it contains must be interpreted restrictively and mainly relate to processing activities that are occasional and non-repetitive<sup>2</sup>.

Moreover, where personal data are transferred to the UK on the basis of Article 46 GDPR safeguards, supplementary measures might be necessary to bring the level of protection of the data transferred up to the EU standard of essential equivalence, in accordance with the Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data<sup>3</sup>.

---

<sup>1</sup> See EDPB information note on BCRs for Groups of undertakings / enterprises which have ICO as BCR Lead SA, [https://edpb.europa.eu/our-work-tools/our-documents/other/information-note-bcrs-groups-undertakings-enterprises-which-have\\_en](https://edpb.europa.eu/our-work-tools/our-documents/other/information-note-bcrs-groups-undertakings-enterprises-which-have_en)

<sup>2</sup> See Guidelines 02/2018 on derogations of Article 49 under Regulation 2016/679, [https://edpb.europa.eu/our-work-tools/our-documents/directrices/guidelines-2018-derogations-article-49-under-regulation\\_en](https://edpb.europa.eu/our-work-tools/our-documents/directrices/guidelines-2018-derogations-article-49-under-regulation_en)

<sup>3</sup> See Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, [https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer\\_en](https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en)

Controllers and/or processors will also need to comply with other obligations deriving from the GDPR, in particular on the need to update the records of processing and privacy notices to mention transfers to the UK.

The EDPB recalls 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.

For data transfers from the UK to the EEA, the EDPB would suggest regularly consulting the UK Government's website and the [ICO's website](#) for up-to-date guidance.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

---

# Information note on data transfers under the GDPR to the United Kingdom after the transition period

Adopted on 15 December 2020

Updated on 13 January 2021

Before the transition period for the United Kingdom's withdrawal from the European Union ended on 31 December 2020, the EU and the UK reached an agreement on 24 December 2020 (the "EU-UK Trade and Cooperation Agreement" or the "Agreement")<sup>1</sup>.

The Agreement was signed by the EU and the UK on 30 December 2020. The EU-UK Trade and Cooperation Agreement started to apply from 1 January 2021 on a provisional basis until 28 February 2021, to provide time to the European Parliament to give its consent on the Agreement and to the Council of the EU to adopt the decision on the conclusion of the Agreement.

The EU-UK Trade and Cooperation Agreement provides that, for a specified period and upon the condition that the UK's current data protection regime stays in place, all transfers of personal data between stakeholders subject to GDPR and UK entities will not be considered as transfers to a third country subject to the provisions of Chapter V GDPR<sup>2</sup>. This interim provision applies from the entry into force of the draft EU-UK Trade and Cooperation Agreement for a maximum period of six months (i.e., until 30 June 2021 at the latest).

This means that organisations subject to GDPR will be able to carry on transferring data to UK organisations without the need to either put in place a transfer tool under Article 46 GDPR or rely on an Article 49 GDPR derogation.

If no adequacy decision applicable to the UK as per Article 45 GDPR is adopted by 30 June 2021 at the latest, all transfers of personal data between stakeholders subject to GDPR and UK entities will then constitute a transfer of personal data to a third country and therefore will be subject to the provisions

---

<sup>1</sup> See EU-UK Trade and Cooperation Agreement, [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22020A1231\(01\)&from=EN](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22020A1231(01)&from=EN)

<sup>2</sup> See Article FINPROV.10A 'Interim provision for transmission of personal data to the United Kingdom', EU-UK Trade and Cooperation Agreement. See also European Commission's Questions & Answers: EU-UK Trade and Cooperation Agreement, under the part on Security, Law Enforcement and Judicial Cooperation in Criminal matters [https://ec.europa.eu/commission/presscorner/detail/en/qanda\\_20\\_2532](https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2532)

of Chapter V GDPR. Therefore, such transfers will require appropriate safeguards (e.g., standard data protection clauses, binding corporate rules<sup>3</sup>, codes of conduct...) with enforceable data subject rights and effective legal remedies for data subjects, in accordance with Article 46 GDPR.

Subject to specific conditions, it may still be possible to transfer personal data to the UK based on a derogation listed in Article 49 GDPR. However, Article 49 GDPR has an exceptional nature and the derogations it contains must be interpreted restrictively and mainly relate to processing activities that are occasional and non-repetitive<sup>4</sup>.

Moreover, where personal data will be transferred to the UK on the basis of Article 46 GDPR safeguards, supplementary measures might be necessary to bring the level of protection of the data transferred up to the EU standard of essential equivalence, in accordance with the Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data<sup>5</sup>.

Controllers and/or processors will also need to comply with other obligations deriving from the GDPR, in particular on the need to update the records of processing and privacy notices to mention transfers to the UK.

The EDPB recalls 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.

For data transfers from the UK to the EEA, the EDPB would suggest regularly consulting the [UK Government's website](#) and the [ICO's website](#) for up-to-date guidance.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

---

<sup>3</sup> See EDPB information note on BCRs for Groups of undertakings / enterprises which have ICO as BCR Lead SA, [https://edpb.europa.eu/our-work-tools/our-documents/other/information-note-bcrs-groups-undertakings-enterprises-which-have\\_en](https://edpb.europa.eu/our-work-tools/our-documents/other/information-note-bcrs-groups-undertakings-enterprises-which-have_en)

<sup>4</sup> See Guidelines 02/2018 on derogations of Article 49 under Regulation 2016/679, [https://edpb.europa.eu/our-work-tools/our-documents/directrices/guidelines-2018-derogations-article-49-under-regulation\\_en](https://edpb.europa.eu/our-work-tools/our-documents/directrices/guidelines-2018-derogations-article-49-under-regulation_en)

<sup>5</sup> See Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, [https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer\\_en](https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en)

## Information note on data transfers under the GDPR to the United States after the adoption of the adequacy decision on 10 July 2023

On 10 July 2023, the European Commission ('the Commission') adopted its 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 ('the Adequacy Decision')<sup>1</sup>, which contains in its annex the EU-US Data Privacy Framework ('DPF').

By doing so, the Commission decided that the United States ('the US'), for the purpose of Article 45 of Regulation (EU) 2016/679 ('the GDPR'), ensures an adequate level of protection for personal data transferred from the EU<sup>2</sup> to organisations in the US that are included in the 'Data Privacy Framework List', maintained and made publicly available by the U.S. Department of Commerce, in accordance with Section I.3 of Annex I of the Adequacy Decision<sup>3</sup>.

Prior to the adoption of this decision, the European Data Protection Board ('the EDPB') adopted its opinion on the draft Adequacy Decision<sup>4</sup>, in compliance with Article 70(1)(s) GDPR.

This document aims at providing some clarity on the implications of the Adequacy Decision for data subjects in the EU and for entities transferring personal data from the EU to the US.

### 1.- How can personal data be transferred to the US on the basis of the DPF?

The Adequacy Decision applies since 10 July 2023. This means that, as of this date, transfers from the EU<sup>5</sup> to organisations in the US that are included in the 'Data Privacy Framework List'<sup>6</sup> may be based on the Adequacy Decision, without the need to rely on Article 46 GDPR transfer tools.

---

<sup>1</sup> 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, C(2023)4745 final.

<sup>2</sup> References to the 'EU' must be understood as references to the EEA/EU.

<sup>3</sup> Article 1 of the Adequacy Decision.

<sup>4</sup> Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework. Adopted on 28 February 2023, [https://edpb.europa.eu/system/files/2023-02/edpb\\_opinion52023\\_eu-us\\_dpf\\_en.pdf](https://edpb.europa.eu/system/files/2023-02/edpb_opinion52023_eu-us_dpf_en.pdf).

<sup>5</sup> This means that the Adequacy Decision does not cover transfers from entities located outside the EU and subject to the GDPR by virtue of Article 3(2) GDPR to organisations in the US that are included in the 'Data Privacy Framework List'.

<sup>6</sup> <https://www.dataprivacyframework.gov/s/participant-search>.

This also means that transfers based on the Adequacy Decision do not have to be complemented by supplementary measures<sup>7</sup>. The EDPB refers to the explanations provided on this matter by the Commission<sup>8</sup>.

## **2.- How can personal data be transferred to the US if the data importer is not included in the ‘Data Privacy Framework List’?**

Transfers to entities in the US which are not included in the ‘Data Privacy Framework List’ cannot be based on the Adequacy Decision and will require appropriate data protection safeguards, enforceable rights and effective legal remedies for data subjects (e.g. through standard data protection clauses, binding corporate rules), in accordance with Article 46 GDPR<sup>9</sup>.

In this respect, the EDPB underlines that all the safeguards that have been put in place by the US Government in the area of national security (including the redress mechanism) apply to all data transferred to the US, regardless of the transfer tool used<sup>10</sup>. Therefore, when assessing the effectiveness of the Article 46 GDPR transfer tool chosen<sup>11</sup>, data exporters should take into account the assessment conducted by the Commission in the Adequacy Decision<sup>12</sup>.

## **3.- Can data subjects in the EU lodge complaints under the DPF?**

Individuals whose data are transferred to the US based on the Adequacy Decision have several redress mechanisms at their disposal if they consider that the US organisation concerned does not comply with the DPF<sup>13</sup>. Individuals are encouraged to first raise any complaint they may have with the relevant US organisation. In case of inquiries, EU organisations may, if necessary, seek the advice of their data protection authorities that are competent to oversee the related processing activities.

## **4. How can EU data subjects make use of the new redress mechanism in the area of national security?**

Regardless of the transfer tool used to transfer their personal data to the US, data subjects in the EU can submit a complaint to their national data protection authority to make use of the new redress mechanism in the area of national security. The national data protection authority, in turn, will ensure that the complaint will be handed over to the EDPB, which will transmit the complaint to the US authorities that are competent to handle the complaint. Furthermore, the data protection authority will ensure that the data subject is provided information regarding the complaint handling process, including with regard to the outcome of the lodged complaint. For a complaint to be admissible,

---

<sup>7</sup> See EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, paragraph 19: [https://edpb.europa.eu/system/files/2021-06/edpb\\_recommendations\\_202001vo.2.0\\_supplementarymeasurestransfertools\\_en.pdf](https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransfertools_en.pdf).

<sup>8</sup> See the Commission’s press release ([https://ec.europa.eu/commission/presscorner/detail/en/ip\\_23\\_3721](https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721)) and Q&A ([https://ec.europa.eu/commission/presscorner/detail/en/qanda\\_23\\_3752](https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752)).

<sup>9</sup> See EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, [https://edpb.europa.eu/system/files/2021-06/edpb\\_recommendations\\_202001vo.2.0\\_supplementarymeasurestransfertools\\_en.pdf](https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransfertools_en.pdf)

<sup>10</sup> See also [https://ec.europa.eu/commission/presscorner/detail/en/qanda\\_23\\_3752](https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752).

<sup>11</sup> See EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, paragraph 30: [https://edpb.europa.eu/system/files/2021-06/edpb\\_recommendations\\_202001vo.2.0\\_supplementarymeasurestransfertools\\_en.pdf](https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransfertools_en.pdf).

<sup>12</sup> See in particular, recitals (6)-(7) of the Adequacy Decision.

<sup>13</sup> The redress mechanisms are described in the Adequacy Decision, Annex I, Section II.7 and III.11 and Annex I to Annex I.

individuals do not need to demonstrate that their data was in fact collected by US intelligence agencies.

### **5.- Will the Adequacy Decision be reviewed?**

The first review of the Adequacy Decision will take place one year after it enters into force, to verify whether all elements have been fully implemented and effective in practice. Following the first review and depending on its outcome, the Commission will decide, in consultation with the EDPB and the EU Member States, on the periodicity of subsequent reviews, which will in any event take place at least every four years<sup>14</sup>. The EDPB and its members stand ready to actively take part in this evaluation.

For the European Data Protection Board

The Chair  
(Anu Talus)

---

<sup>14</sup> Article 3(4) of the Adequacy Decision.

# Information note on BCRs for Groups of undertakings / enterprises which have ICO as BCR Lead SA

**Adopted on 22 July 2020**

This document is without prejudice to the analysis currently undertaken by the EDPB on the consequences of the CJEU judgment *DPC v Facebook Ireland and Schrems*<sup>1</sup> for BCRs as transfer tools.

- **Authorised BCR holders**

From a procedural perspective:

BCR holders having the ICO as the competent Supervisory Authority ("BCR Lead SA") need to put in place all organisational arrangements on the basis of which a new BCR Lead in the EEA may be identified according to the criteria laid down in WP263 rev.01<sup>2</sup>. This change of BCR Lead shall take effect at the latest at the end of the Brexit transition period.

For BCRs already approved under the GDPR, the new BCR Lead SA in the EEA, as the new competent Supervisory Authority ("SA") in accordance with Article 47.1 GDPR, will have to issue a new approval decision following an opinion from the EDPB before the end of the transition period.

For BCRs for which ICO acted as BCR Lead SA under Directive 95/46/EC, no approval will have to be issued by the new BCR Lead SA in the EEA.

From a content perspective:

BCR holders having the ICO as BCR Lead SA need to amend their BCRs with reference to the EEA legal order before the end of the Brexit transition period. To assist Groups of undertakings/enterprises in this process, a checklist of elements to be amended is provided in annex to this note.

In the absence of such changes and/or a new approval, where applicable, before the end of transition period, Groups of undertakings/enterprises will not be able to rely on their BCRs as a valid transfer mechanism for transfers of data outside the EEA after the end of the transition period.

---

<sup>1</sup> CJEU, *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems* (C-311/18).

<sup>2</sup> Article 29 Working Party, Working Document Setting Forth a Co-Operation Procedure for the approval of "Binding Corporate Rules" for controllers and processors under the GDPR, WP263 rev.01, adopted on 11 April 2018 - endorsed by the EDPB.

The EDPB also recalls that following the entry into application of the GDPR two years ago, Groups of undertakings/enterprises should have already updated their BCRs under the GDPR in accordance with the requirements as specified in WP256 rev.01<sup>3</sup> and WP257 rev.01<sup>4</sup>. While the taking over of a BCR by a new BCR Lead SA does not imply that it has verified whether such updates have been made, it remains at any time in a position to do so and to request that relevant changes are made by any BCR holder and adopt any consequent decision in this regard. Any other changes to the BCRs taken over as described above may also be requested if deemed necessary by the new BCR Lead SA. All the SAs, including the new BCR Lead SA, reserve their right to exercise their powers including, the power of conducting an investigation on BCRs, including of the BCR implementation itself, or to give a special attention to certain aspects of such BCR in the context of a broader investigation of the company, and, where appropriate, an approval.

- **Current BCR applications before the ICO**

From a procedural perspective:

Groups of undertakings/enterprises for which BCRs are at the review stage by the ICO are encouraged to put in place all organisational arrangements on the basis of which a new BCR Lead SA in the EEA could be identified according to the criteria laid down in the WP263 rev.01 before the end of the Brexit transition period. They will have to contact this SA in order to provide all necessary information as to why the given SA should be considered as the new BCR Lead SA.

The new BCR Lead SA will take over the application and formally initiate an approval procedure subject to an opinion of the EDPB.

During the transition period, Group of undertakings/enterprises might decide to transfer their BCR application to a new BCR Lead SA after approval by the ICO. In that case, the new BCR Lead SA in the EEA, as the new competent SA in accordance with Article 47.1 GDPR, will have to issue, before the end of the transition period, a new approval decision following an opinion from the EDPB.

From a content perspective:

Any Group of undertakings/enterprises that has BCRs in the process of being approved by the ICO before the end of the transition period following an opinion of the EDPB, must ensure that their BCRs refer to the EEA legal order with information about related changes to become effective (at the latest) at the end of the transition period. To assist them in this process, a checklist of elements to be included is provided in annex to this note.

In both scenarios above, the SA in the EEA that may be approached to act as the new BCR Lead SA will consider, on the basis of criteria set out in WP263 and in cooperation with other concerned SAs, whether it is the appropriate BCR Lead SA on a case-by-case basis and inform the Group accordingly.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

---

<sup>3</sup> Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules as last revised and adopted on 6 February 2018, WP256 rev.01 - endorsed by the EDPB.

<sup>4</sup> Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules as last revised and adopted on 6 February 2018, WP257 rev.01 - endorsed by the EDPB.

## Annex: Checklist of elements for Controller and Processor BCRs which need to be amended for a BCR Lead SA change in the context of Brexit

- The following elements are to be updated due to a BCR Lead SA change in the context of Brexit. In addition to the elements outlined in the table below, all definitions of EEA entities, EEA applicable law and any other relevant definitions should be amended in both BCR for controllers (“BCR-C”) and BCR for processors (“BCR-P”).
- In the specific case of BCR-P, consideration needs to be given to the need to re-word the Service Level Agreement (“SLA”) where the controller is in the UK. Additionally, in BCR-P scenarios where the Group member contracting with the controller is based in the UK, the SLA will need to be re-signed with an EEA-based Group member.

Criteria for a BCR Lead SA change <sup>5</sup>	In the BCRs	In the application form	Text of reference	Comments	Reference to application form / BCRs
<b>1. BINDING NATURE</b>					
1.2 An explanation of how the rules are made binding on the BCR members of the Group of undertakings / enterprises and also the employees	YES  In the BCRs and the documents linked to it, especially the chosen legally binding measures	YES  Section 4 of WP264 <sup>6</sup> or WP265 <sup>7</sup>	Art. 47.1.a and 47.2.c GDPR	<ul style="list-style-type: none"> <li>Duty of the Group of undertakings / enterprises to arrange internal matters in order to ensure that the BCRs will be binding throughout the EEA, e.g.: where necessary, replace any reference to the former ‘BCR applicant (in the UK)’ with the new ‘BCR applicant in the EEA’.</li> <li>If the bindingness is ensured by means of a unilateral</li> </ul>	

<sup>5</sup> Those criteria are those from the WP256rev.01 and WP257rev.01 (endorsed by the EDPB), which the EDPB considers are impacted by Brexit.

<sup>6</sup> Article 29 Working Party, Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, WP264, adopted on 11 April 2018 - endorsed by the EDPB.

<sup>7</sup> Article 29 Working Party, Recommendation on the Standard Application for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, WP265, adopted on 11 April 2018 - endorsed by the EDPB.

Criteria for a BCR Lead SA change <sup>5</sup>	In the BCRs	In the application form	Text of reference	Comments	Reference to application form / BCRs
				<p>declaration, it would be necessary to assess that the participating member of the Group of undertakings / enterprises ('BCR member') making the unilateral declaration is established in a Member State recognising this legal instrument.</p> <ul style="list-style-type: none"> <li>• In the legal instrument used to make the BCR binding, replace any reference to the 'contract law (in the UK)' applicable to the legally binding instrument with the new EEA contract law.</li> <li>• Request the Group of undertakings / enterprises to amend/update all the documents linked to the BCR, especially the chosen legally binding measures (e.g., IGA).</li> </ul>	
<b>EXTERNALLY</b>					
1.3 The creation of third-party beneficiary rights for data subjects. Including the possibility to lodge a	YES	YES	Art. 47.1.b and 47.2.c, 47.2.e GDPR	<ul style="list-style-type: none"> <li>• Ensure that the referred competent SAs are based in the EEA, in line with the</li> </ul>	

Criteria for a BCR Lead SA change <sup>5</sup>	In the BCRs	In the application form	Text of reference	Comments	Reference to application form / BCRs
complaint before the competent SA and before the courts		Section 4 of WP264 and WP265		<p>WP256 rev.01<sup>8</sup> and WP257 rev.01<sup>9</sup>.</p> <ul style="list-style-type: none"> <li>• Ensure that reference is made to EEA-based courts in line with the WP256 rev.01 and WP257 rev.01, including with respect to rights that are enforceable directly against the processor, and rights that are enforceable against the processor when the data subject is not able to bring a claim against the controller.</li> </ul>	
1.4 Responsibility towards the controller	YES (applicable only to BCR-P)	YES (applicable to BCR-P only) Section 4 of WP265	WP257 rev.01 Section 1.4	<ul style="list-style-type: none"> <li>• Ensure that the service agreement used to make the BCR-P binding towards the controller is signed, on the side of the Group of undertakings / enterprises acting as processor, by a BCR member in the EEA.</li> <li>• Ensure that the controller is entitled to enforce the BCR-P</li> </ul>	

<sup>8</sup> Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules as last revised and adopted on 6 February 2018, WP256 rev.01 - endorsed by the EDPB.

<sup>9</sup> Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules as last revised and adopted on 6 February 2018, WP257 rev.01 - endorsed by the EDPB.

Criteria for a BCR Lead SA change <sup>5</sup>	In the BCRs	In the application form	Text of reference	Comments	Reference to application form / BCRs
				against at least one BCR member in the EEA (i.e., either a BCR member with delegated data protection responsibilities in the EEA, or the EEA exporter).	
1.5 The EU headquarters, EU member with delegated data protection responsibilities or the data exporter accepts liability for paying compensation and to remedy breaches of the BCRs	YES	YES Section 1, 3, and 4 of WP264 and WP265	Art. 47.2.f GDPR	<ul style="list-style-type: none"> <li>Where the BCR member with delegated responsibilities was one based in the UK, the new entity taking liability for any violations of the BCRs by other BCR members outside of the EEA shall be located in the EEA.</li> <li>Furthermore, as a reminder, where the BCRs provide that every BCR member exporting data out of the EEA on the basis of the BCRs will be liable for breaches of the BCRs by the data importer, the BCR member located in the UK shall be considered a data importer and not a data exporter.</li> </ul>	
1.6. The company has sufficient assets.	NO	YES	Art. 47.2.f GDPR	<ul style="list-style-type: none"> <li>Provide confirmation of whether the new entity taking liability in the EEA has</li> </ul>	

Criteria for a BCR Lead SA change <sup>5</sup>	In the BCRs	In the application form	Text of reference	Comments	Reference to application form / BCRs
		Section 4 of WP264 and WP265		sufficient financial means (or confirmation of an insurance) to cover any damages.	
<b>2. EFFECTIVENESS</b>					
2. The existence of a complaint handling process for the BCRs.	YES	YES Section 5 of WP264 and WP265	Art. 47.2.i and Art 12.3. GDPR	<ul style="list-style-type: none"> <li>• Ensure that any reference to the competent SA refers to EEA SAs (choice before the SA in the EEA State of his habitual residence, place of work or place of the alleged infringement in the EEA, pursuant to Art. 77 GDPR).</li> <li>• Ensure that any reference to the ‘competent courts’ or ‘national jurisdiction’ will be based in the EEA (choice for the data subject to act before the EEA courts where the controller or processor has an establishment or where the data subject has his or her EEA habitual residence pursuant to Art. 79 GDPR).</li> </ul>	
2.3. The existence of an audit programme covering the BCRs.	YES	YES	Art. 47.2.j; Art 47.2.l and Art. 38.3 GDPR	Ensure that the SAs having received the authority/power to carry out a data protection audit	

Criteria for a BCR Lead SA change <sup>5</sup>	In the BCRs	In the application form	Text of reference	Comments	Reference to application form / BCRs
		Section 5 of WP264 and WP265		<p>of any BCR are based in the EEA.</p> <ul style="list-style-type: none"> <li>Replace any reference to the former BCR Lead SA (in the UK) with the new one.</li> </ul>	
<b>3. COOPERATION DUTY</b>					
3.1. A duty to cooperate with SAs.	YES	YES Section 6 of WP264 and WP265	GDPR Art. 47.2.l.	<ul style="list-style-type: none"> <li>Ensure that the duty to cooperate with the SAs is referring to SAs based in the EEA.</li> </ul>	
3.2 A duty to cooperate with the controller.	YES (applicable only to BCR-P)	YES (applicable to BCR-P only) Section 7 of WP265	WP257rev.01 Section 3.2	<ul style="list-style-type: none"> <li>Ensure that the duty to cooperate with the SAs is referring to SAs based in the EEA.</li> </ul>	
<b>4. DESCRIPTION OF PROCESSING AND DATA FLOWS</b>					
4.1. A description of the material scope of the BCRs (nature of data transferred, type of data subjects, countries).	YES	YES Section 2, 3, and 7 of WP264 and Section 2, 3, and 8 of WP265	Art. 47.2.b GDPR	<ul style="list-style-type: none"> <li>Remove the UK from the list of 'EEA Member States'.</li> <li>Add the UK to the list of third countries to which personal data will be transferred (if applicable) and remove UK entities from the list of exporters.</li> </ul>	

Criteria for a BCR Lead SA change <sup>5</sup>	In the BCRs	In the application form	Text of reference	Comments	Reference to application form / BCRs
4.2. A statement of the geographical scope of the BCRs.	YES	YES Section 2 and 7 of WP264 and Section 2 and 8 of WP265	Art. 47.2.a GDPR	<ul style="list-style-type: none"> <li>Add the UK to the list of third countries and remove UK entities from the list of exporters.</li> </ul>	
<b>5. MECHANISMS FOR REPORTING AND RECORDING CHANGES</b>					
5.1. A process for updating the BCRs.	YES	YES Section 8 of WP264 and WP265	Art. 47.2.k GDPR	<ul style="list-style-type: none"> <li>Replace any reference to the former BCR Lead SA (in the UK) with the new one in the EEA.</li> </ul>	
<b>6. DATA PROTECTION SAFEGUARDS</b>					
6.1.2. Accountability and other tools.	YES	YES Section 10 of WP264 and WP265	Art. 47.2.d and Art. 30 GDPR	<ul style="list-style-type: none"> <li>Ensure that any reference to SAs is to be understood as EEA SAs.</li> </ul>	
6.3. A need to be transparent where national legislation prevents the group from complying with the BCRs.	YES	NO	Art. 47.2.m GDPR	<ul style="list-style-type: none"> <li>Ensure that the reporting duty will be made to EEA SAs.</li> </ul>	

# Internal EDPB Documents



## **EDPB Best practices for the organisation of EDPB Plenary meetings**

**Adopted on 14 November 2023**

## Table of contents

1	Purpose and scope.....	3
2	Roles and responsibilities.....	3
3	Plenary agendas .....	4
3.1	Scheduling.....	4
3.2	Submission of agenda items and circulation of documents.....	4
3.3	Structure of the agenda.....	4
4	Written Procedure .....	6
5	Maturity of Agenda Items.....	7
5.1	Focus of the Plenary .....	7
5.2	Info notes.....	7
5.3	Requests for mandates.....	8
6	Plenary discussions .....	8
6.1	Structure of the discussions .....	8
6.2	Scope of the discussions.....	9
7	Outcome of the Plenary.....	9
8	Periodic evaluation .....	9

# **The European Data Protection Board**

Having regard to Article 68 and Article 70 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 2, 3, 18, 19 20, 22, 24, 25, 26, 27 and 28 of its Rules of Procedure “RoP” as amended on 23 November 2018,

## **HAS ADOPTED THE FOLLOWING INTERNAL BEST PRACTICES**

### **EDPB BEST PRACTICES ON ORGANISATION OF ITS PLENARY MEETINGS**

## **1 PURPOSE AND SCOPE**

1. This document aims at providing guidance on how the EDPB Plenary meetings should be organised, considering in particular its interaction with the EDPB Expert Subgroup (ESG) and Taskforce (TF) meetings. Specifically, the objectives of this document are to focus and prioritise the work of the Plenary, to improve the flow and sharing of information and to increase the efficiency of the plenary meetings.

## **2 ROLES AND RESPONSIBILITIES**

2. The Board is tasked with ensuring the consistent application of applicable EU data protection laws, by performing a number of tasks pursuant to Article 70 of the GDPR and Article 2 of EDPB RoP.
3. The Plenary meetings are responsible for:
  - i. Discussing developments or policy questions in relation to issues of significant strategic importance and deciding on any necessary action required;
  - ii. Giving mandates to ESGs, TFs or the EDPB Secretariat;
  - iii. Receiving information and state of play updates on the progress of the work made by ESGs, TFs or the EDPB Secretariat;
  - iv. Giving directions to the ESGs, TFs or the EDPB Secretariat and deciding on concrete proposals and options prepared by them (see also Article 28.2 RoP); and
  - v. Adopting EDPB documents, generally prepared by the ESGs, TFs or the EDPB Secretariat.
4. In this context, the Plenary will generally have a more strategic, policy and high-level focus compared to the ESGs and TFs, who may explore issues more extensively in order to prepare, inform and support the Plenary’s decisions.

## 3 PLENARY AGENDAS

### 3.1 Scheduling

5. Without prejudice to extraordinary meetings that may take place due to unforeseen and unplanned circumstances, the meetings should in principle take place every month.

### 3.2 Submission of agenda items and circulation of documents

6. As regards the submission of agenda items, the estimated time that will be needed for discussion, should be indicated by the coordinator(s)/rapporteurs(s) at the moment of the submission. The agenda can then be prepared accordingly.
7. Submissions of items for the agenda of Plenary meetings must respect the established deadlines communicated by the Secretariat. Exceptionally, when rapporteur(s) or coordinator(s) know that documents will be late for circulation to the members, they should inform the Chair and the Secretariat in advance and explain the reason for such late submission. Unless there is a specific need of urgency, items submitted after the deadline should not be taken into account for the specific Plenary meeting and may need to be resubmitted for a subsequent meeting.
8. Article 19(1) of the RoP sets out the deadlines for circulating the agenda of the upcoming Plenary meetings to the members of the Board. Similarly, Article 20(1) of the RoP sets out the deadlines for circulating the corresponding documents.

### 3.3 Structure of the agenda

9. The agenda of plenary meetings should be divided into the following parts<sup>1</sup>:

#### **Point A: Adoption with no discussion<sup>2</sup>**

10. The document is fully ready for adoption, with a consensus at the ESG or TF level if relevant. In this case, in principle neither presentation nor discussion at the Plenary will be necessary. Requests for mandates enjoying consensus at ESG or TF level and which relate to items already listed in the EDPB strategy and work plan<sup>3</sup> shall in principle be placed on the agenda as point A items. The same applies for recurrent Article 64 (1) GDPR opinions, such as on BCR or on the requirements for accreditation of code of conduct monitoring bodies or certification bodies.<sup>4</sup> Strategically important documents should not be placed under point A, even if they enjoy consensus.<sup>5</sup>

---

<sup>1</sup> While respecting those four parts, the Chair and EDPB Secretariat should make its best effort to combine items observers can attend, while bearing in mind also the need to smoothly and effectively structure the agenda.

<sup>2</sup> There will be no discussion in principle. If an EDPB member requests an item to be discussed, this item will remain in Point A, but will be flagged for discussion.

<sup>3</sup> See the additional condition under section 5.4(i) of the present Document to have at least a lead rapporteur.

<sup>4</sup> Documents enjoying consensus at the ESG or TF level could also be adopted via written procedure instead, which would mean that they would not be part of the Plenary agenda (see section 4 below).

<sup>5</sup> Strategically important documents may for example include adoption of an opinion under Article 64(2), a binding decision pursuant to Article 65(1), EDPB-EDPS Joint Opinions, or new guidelines.

11. The EDPB Secretariat will circulate the draft agenda and the respective, above-mentioned documents to the EDPB participants<sup>6</sup> in line with the deadlines set out in the RoP.<sup>7</sup> The agenda items under point A shall be submitted, together, to a single vote.
12. During the voting procedure, the Chair will ask who is in favour of adopting all the items put forward for adoption without discussion. The Chair then asks if there are any votes against or abstentions. Should that be the case, the EDPB member(s) in question will have the opportunity to specify to which document the vote against or abstention relates so that this can be noted by the EDPB Secretariat.
13. However, any EDPB participant may, at any time before the adoption of the agenda, ask the Chair to disjoin a draft which, in its view, should be debated or amended. This participant should share this request as soon as possible and should indicate the specific issue that needs to be discussed in order to enable the other participants to be prepared for the discussion. The disjoined draft will remain under point A, but will be flagged as being subject to a specific debate and vote, and if needed, may be placed on the agenda of one of the following Plenary sessions.

## **Point B: Discussion**

### **B1: Discussion with a view to adoption**

14. The document is in principle ready for adoption, but might still require a final decision on strategic issues clearly defined as requiring arbitration. The EDPB members are requested to decide on the matters identified for discussion, on the basis of the concrete options precisely described in the info note. The Plenary nevertheless remains free to combine the options proposed or to choose another one.

### **B2: Policy debate**

15. This point allows for the involvement of the EDPB participants in policy debates. Questions can be referred to the Plenary if there is a need for strategic direction to facilitate the finalisation of a document, or if it is deemed useful to hold a policy debate on another pressing issue at Plenary level.<sup>8</sup> During the discussion of agenda items under this point, all the attending EDPB participants are encouraged to share their views (including by supporting another participant).
16. When a strategic item is ready for discussion, the lead rapporteur, together with the competent ESG or TF Coordinator(s), should assess whether the discussion is better suited for the Plenary, for the Strategic Advisory Expert Subgroup, or at the level of the other ESGs or TFs. Unless the latter is the case, the Chair should be contacted via the EDPB Secretariat, so that the Chair can take a decision.

---

<sup>6</sup> EDPB participants, in the context of this Document, shall mean participants to plenary meetings: EDPB members, observers, the EFTA Surveillance Authority, the European Commission and the EDPB Secretariat. This is without prejudice to rules on confidentiality which may restrict participation by observers in certain matters and agenda items.

<sup>7</sup> The circulation of documents to the observers depend on the scope of their right as observer and on the applicable confidentiality rules.

<sup>8</sup> Where necessary, a Strategic Advisory ESG meeting should be set up before the Plenary meeting to discuss important strategic matters. This could for example be the case when legal deadlines are applicable (e.g. Article 65 decisions – dispute resolution procedure) or when there is a need to organise an in-depth discussion at a higher, more strategic level than the level of the other ESGs or TFs, and the rapporteurs need those decisions to finalise the document for the Plenary meeting.

### **Point C: Organisational matters**

17. This point will cover organisational matters such as i) designation/renewal of coordinators by the EDPB; ii) announcement of ad hoc Plenaries; iii) announcement of the new Commissioners or departures, etc.

### **Point D: Information**

#### **Point D1: Outcome of written procedures or urgent decisions**

18. The outcome of any written procedures or urgent decisions taken by the Chair since the last Plenary will be placed under this point of the agenda and recorded in the minutes.

#### **Point D2: Updates by EDPB participants**

19. Where EDPB participants wish to share important information points of general interest that are relevant for the Plenary (e.g., recent developments at national level and important ongoing projects), they are invited to request it to be added under this section.<sup>9</sup> Such information should be provided briefly. EDPB participants remain free to consider other appropriate channels to share their information points, such as via the most relevant ESG, TF or in written form. An info note should in principle be provided for D2 points. Except for important urgent matters, this section cannot be used to request new mandates.<sup>10</sup>

#### **Point D3: AOB**

20. EDPB participants can request to add an AOB point in case they wish to share orally important information of relevance for the EDPB participants for which no written information has been shared in advance, for example due to the proximity of the reported event with the meeting. They should still consider whether information can be shared with the other participants ahead of the meeting, and the oral intervention can also be supplemented with written information afterwards as appropriate.

### **Point E: Written stay of play**

21. Documents shared only for information. In principle no discussion is expected on these documents, unless a participant has comments to the documents shared. In this case, any participant should be able to share its comments orally during the meeting.

## **4 WRITTEN PROCEDURE**

22. Except for strategically important documents, where a document is ready for adoption and supported by consensus, it will normally be placed under point A of the Plenary agenda, as explained above under point 3.3. This will ensure maximum transparency towards the public, who can access the Plenary agenda or press release.

---

<sup>9</sup> Information shared on important cases by members during the Plenary meeting does not replace the need to share information in the Enforcement ESG as well as, for cases subject to cooperation, via IMI.

<sup>10</sup> Any request of mandate should respect the conditions of section 5.4 below.

23. However, there may be an urgent need to adopt such a document, and it may not be feasible to organise an *ad hoc* Plenary accordingly. In this case, the rapporteur(s) and/or Coordinator(s) may propose to request the Chair or the Board for an adoption by written procedure. Following this, the coordinator(s) will notify the EDPB Secretariat about this request and will submit it for the Chair's approval. According to Article 24 RoP, it is also possible for the Board to decide on the launching of a written procedure.
24. Before the document is submitted for adoption via written procedure, the Secretariat circulates it among the members and indicates a specific deadline, as decided by the Chair, until when the members may provide final written comments. This ensures that all members, including those not taking part in a particular ESG or TF activity if relevant, have the opportunity to comment on the document before voting.
25. During this stage, final comments may be put forward. The rapporteurs should assess whether these comments indicate that the document is not supported by general consensus or that it has not yet reached a sufficient level of maturity for adoption, or whether the comments can be easily resolved so that written procedure can be launched by the EDPB Secretariat upon the Chair's decision.<sup>11</sup>
26. The EDPB Secretariat will inform the EDPB members and the relevant ESG or TF of the results of the written procedure.

## 5 MATURITY OF AGENDA ITEMS

### 5.1 Focus of the Plenary

27. In order to enable an efficient functioning of the Plenary meetings, the Plenary should only address work items that are sufficiently prepared. If the Plenary considers that an agenda item lacks the sufficient level of maturity, it may choose to postpone the agenda item until the necessary amendments have been carried out. Participants attending the discussions in the Plenary should also ensure they are well prepared and informed on the work items discussed in the Plenary. The Plenary should focus on the discussion points identified in advance, as provided in the respective info note.

### 5.2 Info notes

28. In line with Article 20(2) RoP, all Plenary agenda items, both under point A, B and D, shall have an info note accompanying them. An exemption may apply for urgency procedures of Article 66 GDPR. For C points, an info note should in principle accompany them.
29. An info note should be as brief as possible, and it should include the following elements:
  - i. The background of the agenda item, shortly outlined;

---

<sup>11</sup> Article 24(4)–(6) RoP sets out the rules for suspension of a written procedure once initiated. Members who disagree with the adoption of a document may vote against it during the written procedure.

- ii. A short summary of the document and its main objectives, where appropriate;<sup>12</sup>
  - iii. Any discussion that took place during the drafting for which a participant flagged their intention to still raise the issue at Plenary level and shared its view succinctly in writing;
  - iv. The discussion points, clearly explained, with concrete options to decide between together with an explanation of their strategic consequences, in line with Article 28 RoP; and
  - v. If relevant, it may include the results of the indicative votes expressed during the detailed drafting discussions of the document (i.e., in an ESG or a TF), where appropriate.
30. Info notes should be prepared by the lead rapporteur with the input of the other rapporteurs, the Coordinator(s) and the EDPB Secretariat.

### 5.3 Requests for mandates

- i. Any request for mandate shall be provided in writing and include at least a lead rapporteur. Without lead rapporteur, the request shall not be made;
- ii. Any request for mandate shall be motivated and underline the level of importance to deal with the issue. The request should also highlight the relationship between the topic and the EDPB Strategy and the EDPB Work Programme, and, where this relationship is not identifiable, explain why the mandate should be granted nevertheless;
- iii. Any request for mandates should include an indication of the timeline for delivery of results;
- iv. Where possible and feasible, any request for mandates should be first discussed in an ESG or TF. The relevant ESG or TF Coordinator(s) and the EDPB Secretariat will assess the request, consider its level of importance, evaluate it in light of the EDPB Strategy and the workload at the ESG or TF level, and make a proposal to the Plenary meeting to either adopt or refuse the request. If the level of importance is high, but the workload of the respective ESG or TF is heavy, the EDPB Secretariat and the Coordinator will discuss how this mandate will impact the other work items currently dealt with by the ESG or TF and which of them should be de-prioritised;
- v. Unless requests for mandate are dealt with via a written procedure, requests for mandates enjoying consensus at ESG or TF level and relating to items already listed in the EDPB strategy and work plan will generally be placed on the Plenary meeting agenda as point A items (Adoption with no discussion) unless a discussion is necessary, in which case it would normally be put under point B of the agenda.

## 6 PLENARY DISCUSSIONS

### 6.1 Structure of the discussions

31. Discussions at Plenary level should be structured as follows:
- i. Brief presentation by the rapporteur(s)<sup>13</sup>, focusing on the specific issues for arbitration/discussion;
  - ii. EDPB participants indicate their intention to react by raising their signs;
  - iii. The Chair should ensure that all participants can intervene and that the distribution of interventions remains fair and balanced. For each item of discussion, the Chair should allocate

---

<sup>12</sup> This short summary is not needed for short documents as letters and for guidelines for which an executive summary is provided.

<sup>13</sup> Could be the ESG or TF Coordinator(s) or one of the rapporteurs of the file.

a maximum speaking time to participants for their respective interventions – for instance, depending on the circumstances, it may be appropriate to ask participants to aim to limit their intervention to two minutes. In any case, the allocated speaking time should always take into account the topic at hand and the foreseen duration of the discussion in the agenda.

32. The discussion should facilitate the exchange of views between all EDPB participants with an opinion on the matter in a timely manner.

## 6.2 Scope of the discussions

33. In principle, to the extent possible, all comments of the participants should be made and addressed in advance of the Plenary. This allows the Plenary to focus on the discussion points identified as requiring the Plenary's attention. Any discussion at this point should aim at solving matters of strategic importance on which the ESG, TF or drafting team could not find an agreement. Those matters, clear options to decide between, and the results of any indicative votes should be described in detail in the info note as outlined above in point 5.2.
34. Where there are different options to decide between, those will be specified in the info note. To the extent possible, the Plenary should in principle avoid deciding between more than two options at a time so as to facilitate the reaching of a majority. The Plenary nevertheless remains free to combine the options proposed or to choose another one.
35. Where necessary, the EDPB participants should not be prevented from raising new issues at Plenary level, in particular where they did not have the opportunity to raise them earlier. Any issue should be raised as soon as possible to ensure that the other EDPB participants as well the rapporteurs can be fully prepared for the discussions.

## 7 OUTCOME OF THE PLENARY

36. After the Plenary, the EDPB Secretariat will circulate a draft press release to be circulated to the EDPB Communications Network. A deadline for feedback will be indicated by the EDPB Secretariat. After the approval of the Chair, the press release will be published on the EDPB website.
37. Before any documents adopted by the EDPB Plenary can be published, the EDPB Secretariat, in liaison with the rapporteurs where necessary, will proofread the documents and carry out editorial changes as necessary.

## 8 PERIODIC EVALUATION

38. Once adopted, these best practices should apply for a pilot period of six months. The Plenary will decide after this period whether to keep the present Best practices and whether adjustments to the Best practices are necessary.
39. If the pilot phase proves successful and the best practices are maintained, periodic evaluations of working methods should be carried out once every three years unless the Plenary decides

otherwise. Evaluations should be supported by surveys, which can be anonymous. The surveys should be based on metrics that allow for comparisons to be made over time.

For the European Data Protection Board  
The Chair  
(Anu Talus)

# EDPB Documents



## PROCESS GUIDE FOR THE SELECTION AND THE HANDLING OF STRATEGIC CASES

**Version 2**

### INTRODUCTION

At a two-day high-level meeting in Vienna in April 2022, EDPB members agreed to further enhance cooperation on cases of strategic importance (hereafter “strategic cases”), and to diversify the range of cooperation methods used to handle them. In particular, it was decided that EDPB members will 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.

In line with the Statement on enforcement cooperation adopted at the Vienna meeting by EDPB members<sup>1</sup>, this process guide aims at (i) specifying the criteria and the selection process allowing the identification of “strategic cases” and (ii) to detail how EDPB members can handle these strategic cases through the enhanced cooperation mechanism.

It should be noted that cases of strategic importance should, in principle and by priority, be one-stop-shop cases and that they should be handled following a flexible and pragmatic approach, in the spirit of good cooperation between supervisory authorities (hereafter “SA’s”). In the same spirit, SA’s will exchange information and cooperate in informal ways at the different stages specified below when handling strategic cases.

Lastly, it should be noted that the handling of cases of strategic importance will eventually take place in accordance with - and by making full use of - the procedures and instruments for achieving cooperation and consistency between SA’s, as laid down in Chapter VII of the GDPR.

---

<sup>1</sup> Statement on enforcement cooperation, EDPB, on 28<sup>th</sup> April 2022, [here](#).

## I. SELECTION OF CASES OF STRATEGIC IMPORTANCE BY THE EDPB

The aim of this section is to specify the criteria that define a case of strategic importance, as well as to detail the procedures that should be followed, from the identification of a case of strategic importance by an SA until its qualification as strategic case by the EDPB.

### 1. Criteria to prioritise case of strategic importance

The paragraphs below lay down criteria to assess whether or not a case qualifies as a strategic case in accordance with the Statement on enforcement cooperation made by the EDPB at the Vienna meeting in 2022.

First of all, a strategic case should be a case where it is likely that a high risk to the rights and freedoms of natural persons in several Member States exists. Therefore, this subsection aims at listing criteria that contribute, individually and/or cumulatively, to discerning whether a case represents a high risk to the rights and freedoms of the data subjects.

To identify potential strategic case, an SA can base its proposal on the following list of criteria:

- A **structural or recurring problem** in several Member States in particular where the case concerns a general legal issue with regards to the interpretation, application or enforcement of the GDPR;
- A case related to the **intersection of data protection with other legal fields**;
- A case which affects a **large number of data subjects** in several Member States;
- A **large number of complaints** in several Member States;
- A **fundamental issue falling within the scope of the EDPB strategy**;
- A case **where the GDPR implies that a high risk can be assumed**, such as:
  - The processing of special categories of data as referred to in Articles 9 and 10 of the GDPR;
  - A processing regarding vulnerable people such as minors;
  - Situations mentioned in Article 35 (3) of the GDPR where a data protection impact assessment (DPIA) is required, or situations where a DPIA is required based on the criteria<sup>2</sup> for processing operations that are likely to result in a high risk as laid down in the Guidelines on Data Protection Impact Assessment<sup>3</sup>.

---

<sup>2</sup> These criteria are: 1) Evaluation or scoring, including profiling and predicting 2) Automated-decision making with legal or similar significant effect 3) Systematic monitoring 4) Sensitive data or data of a highly personal nature 5) Data processed on a large scale 6) Matching or combining datasets 7) Data concerning vulnerable data subjects 8) Innovative use or applying new technological or organisational solutions 9) When the processing in itself “prevents data subjects from exercising a right or using a service or a contract”.

<sup>3</sup> Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248rev.01, as endorsed by the EDPB on 25 May 2018.

Any case that meets at least one of the criteria listed above could be submitted as a potential strategic case to the other EDPB members. While it is sufficient for a strategic case to meet only one of criteria listed above, the EDPB members could also take into consideration the total number of criteria that are met in the proposal when selecting strategic cases to be submitted to the PLEN. It should be noted that the list of criteria is not exhaustive and that SAs may include additional reasoning in their proposals.

Finally, it should be noted that the degree of public debate and media attention are not included as relevant criteria. These audience factors should nevertheless be considered by the EDPB members when selecting a case.

## 2. Process and timeline for the selection of cases by the EDPB

This subsection lays out the essential steps from the identification of a case that could potentially become a strategic case to its submission to the Plenary for adoption.

### 2.1. Identification of a case by SA and submission to the ENF subgroup

On a voluntary basis, any SAs convinced that one of the criteria listed above is fulfilled for a case is allowed to submit a proposal of strategic case to the ENF subgroup.

More specifically, proposals of case of strategic importance can be submitted:

- Either by the lead supervisory authority (hereafter “LSA”), for instance where it needs technical support or investigations to be carried out;
- Or by a concerned supervisory authority (hereafter “CSA”) to prioritize the work on a specific case where it is not the LSA.

The EDPB will not decide that a case should be designated as a “strategic case” without the agreement of the LSA. Where a CSA wants to submit a strategic case for discussion before the EDPB, they should ideally seek the approval of the LSA first, both in line with the spirit of good cooperation and considering that the submission of a case as a possible strategic case could potentially create procedural difficulties for the LSA in a case that they are handling. However, although the LSA’s approval is required for the selection of a case as strategic, and while the LSA’s approval is preferable before a case is submitted for selection as a strategic case, the LSA’s approval is not required before the EDPB discuss a case for selection.

To submit a proposal to the ENF subgroup, the SA should complete the standard form at the end of this process guide and detail the criteria met by the case, the reasons of its proposal, and a proposed timetable/estimated deadline for the handling of the case.

### 2.2. Preselection of potential strategic cases by the ENF subgroup

Before its submission to the Plenary, the proposal supported by a supervisory authority should be submitted for discussion to the ENF subgroup. The proposal remains a “potential” strategic case until its adoption by the Plenary.

The supervisory authority submitting a case of strategic importance should transmit its proposal sufficiently in advance of the ENF subgroup meeting to leave time for every SA to analyze the potential strategic cases on the agenda before the meeting, to ensure informed discussions.

During this ad hoc ENF ESG meeting, the EDPB members discuss the submitted case(s) based on their analysis, with the aim to identify among the potential strategic cases, those that could be submitted to the PLEN for adoption, along with proposals for members to be part of the working teams on each case. Again, the selection of cases of strategic importance for which cooperation will be prioritized will be done by the ENF subgroup on the basis of the criteria defined in the previous section.

In order to divide the work and to be able to actually achieve the desired results within the agreed timeframe, the ENF member should remember that the selected cases should be divided over different LSAs and CSAs.

Finally, in order to ensure efficient engagement in the progress of strategic cases, the ENF subgroup should not deal with more than 5 on-going cases at a time (including cases that are not finalized), and therefore should limit the number of cases they select.

### 2.3. Submission and selection of strategic cases to the EDPB

After submission of the potential strategic case by the ENF subgroup to the Plenary for their adoption, the PLEN should decide on the following items:

- whether or not the submitted potential strategic cases should be included in the set of strategic cases cooperation mechanism;
- which authorities will compose the working team on each case and which SA will be in charge to coordinate the group (it should preferably be a small team of 3/4 authorities and should in OSS cases, include the LSA but does not have to include every CSA in order to remain agile);
- regular consultations with the CSAs not in the working team will be held to report on the progress of the work and to submit key points for arbitration, if necessary through the PLEN;
- take note of the work plan on which each case should be processed under the direction of the LSA (delays for investigations, for deliverables...) within a fixed timeline, which in principle should not go beyond 2 years.

After the PLEN meeting, the potential strategic case that has been adopted by the PLEN is qualified as a case of strategic importance at European level. The work team will have to follow the principles and the *modus operandi* detailed in section 2 of this process guide.

## II. WORKING ON A STRATEGIC CASE

This section lays out guidance for the practical implementation of investigations<sup>4</sup> for the SAs involved once a case has been designated as strategic. The handling of strategic case should be guided by the over-arching objectives of the Vienna Process: enhanced cooperation, efficiency and acceleration of investigations.

### 1. General Principles

The pursuit of the objectives of enhanced cooperation and timely investigation should be flanked by the following principles: self-commitment, prioritisation, foresight, transparency, collegiality and pragmatism:

#### 1.1. Self-commitment

Considering the independence of SAs during an OSS procedure and the voluntary nature of the strategic cases process, the adherence to the goals, principles and working methods in this guide shall be understood as an expression of *self-commitment* of the SAs involved to investigate a strategic case in an efficient and timely manner in a spirit of sincere cooperation<sup>5</sup> and the self-set goals expressed in the Vienna Statement. This guide does not prescribe strict or granular procedural rules. Rather, it encourages the SAs involved to set themselves specific goals and methods and to commit to those in each individual case.

#### 1.2. Prioritisation

The notion of “strategic” already implies that such a case should be treated differently from a “normal” case. The high significance of a strategic case (as laid out by the selection criteria in section I.2.) results in the need of SAs to “prioritise” strategic cases, as explicitly mentioned in the Vienna Statement. *Prioritisation* may manifest itself in different forms. First, it can mean that *more* human or financial resources are dedicated towards the case, e.g. in the form of FTE working days. However, acknowledging that resources can be limited by budgetary or other constraints<sup>6</sup>, *prioritisation* need not necessarily result in “extra” resources. SAs could also prioritise by shifting or allocating *existing* resources, e.g. by deciding that a strategic case should be handled by the responsible staff *before* other cases. Third, *prioritisation* may manifest itself through structural and organisational manners within an SA, e.g. by creating expert task forces or by involving senior officials early on in the process. In line with the principle of *self-commitment*, SAs should *prioritise* the handling of strategic cases but they should decide themselves *how* such prioritisation shall take place.

#### 1.3. Foresight

The effective handing of cases of strategic importance further requires *foresight*. SAs should be mindful that an efficient handling of a strategic case can set a precedent and thus lead to more legal certainty and facilitate or avoid the handling of similar cases, thus saving resources,

---

<sup>4</sup> “Investigations” should be understood in a broad sense and should cover both complaint-based as well as ex officio cases within the meaning of Art. 57(1)(f),(h) GDPR.

<sup>5</sup> Art. 4(3) Treaty on European Union.

<sup>6</sup> Possibly reference to contribution to Art. 97 evaluation where lack of resources is mentioned.

especially when the case deals with a structural or recurring problem in several member states. SAs should be aware of what other authorities (e.g. consumer and competition authorities) are doing in parallel. Furthermore, the SAs should anticipate new technical or political developments. The SAs involved should be aware of existing and upcoming guidelines, opinions and other work of the EDPB in such strategic matters.

#### 1.4. Collegiality

SAs should be committed to good cooperation in a spirit of *collegiality*. The EDPB recalls that the key concepts of the cooperation procedure consist of “*an endeavour to reach consensus*” and the obligation to “*exchange all relevant information*”.<sup>7</sup> It is therefore of utmost importance that the SAs cooperate in a collegial manner and all pursue the same objectives within a case, i.e. to swiftly and strongly protecting citizens’ fundamental rights in a consistent manner throughout the entire EEA.

During the whole cooperation procedure all SAs should keep a mindset that all SAs “gain” in the end because the important OSS-case was completed successfully within a reasonable timeframe and setting precedents in landmark decisions will facilitate the handling of future cases. Further, the likelihood of an Article 65 procedure could be decreased.

#### 1.5. Transparency

To succeed in the “*endeavour to reach consensus*” SAs are obliged to “*exchange all relevant information*”<sup>8</sup>. *Transparency* is particularly important in strategic cases, since those are usually quite complex, so early and continuous access to all relevant information is the key to a good collegial cooperation. “*Relevant information*” should be understood in a broad manner. The LSA when it considers it useful for the SAs involved could share details of the investigation beyond the basic information, for example minutes of meetings with the controller or information relating to the technical aspects of the investigation.

*Transparency* does not only pertain to the content of the investigation itself but also to the organisational methods and means of cooperation specific to the strategic nature of the case. Each SA involved shall communicate very clearly, *how* they prioritise the work on the case of strategic importance. Self-set goals, milestones and timetables, and possibly other unique working methods of handling the case should be clearly communicated to the other SAs involved. At the beginning of the investigation, the SAs should engage in discussions in a transparent manner in order to enable the LSA to prioritize certain aspect of the investigation and to draft a timetable of the steps it intends to take within the investigation. Transparency within the cooperation procedure enables the SAs to identify controversial or divergent assessments of facts or legal views as early as possible. This helps to prevent discussions at a later of the procedure and avoids Article 65 procedure. Finally, SAs should be transparent with the public in accordance with applicable national and EU laws<sup>9</sup>.

---

<sup>7</sup> Paragraph 37 of the Guidelines 02/2022 on the application of Article 60 GDPR.

<sup>8</sup> Paragraph 37 of the Guidelines 02/2022 on the application of Article 60 GDPR.

<sup>9</sup> This aspect is more concretely dealt with in Section 5.

## 1.6. Pragmatism and informal communication

In order to improve the cooperation in cases of strategic importance the case handling should be *pragmatic* and tailored towards the specific case. The SAs should focus on the objective of strong and swift enforcement and avoid unnecessary formalism in the cooperation between SAs. That is especially true with regard to means of communication. Here, SAs should not be limited to the use IMI but may resort to more informal and flexible tools. Self-set milestones may be adapted with regard to the overall objectives but shall be communicated with the other SAs involved and the ENF ESG. The discretionary power that SAs enjoy pursuant to domestic law should be exercised in a pragmatic way in order to facilitate and promote the cooperation in the case of strategic importance. In their discussions, the SAs should focus on the essential aspects that are decisive to the outcome of the case in order to ensure a strong and swift enforcement.

## 2. Making a Plan / MoU

In the Vienna statement, the EDPB stated that under the direction of the LSA, an action plan will be established to ensure that the work will be conducted in the most efficient manner and within a fixed timeline. The following sections should be understood as a best practice. However, with respect to the principle of pragmatism, SAs are free to deviate from the suggested approach if necessary.

### 2.1. Kick-off Meeting with LSA + dedicated CSAs (“working team”)

That requires an *early* exchange between the LSA and the dedicated CSAs (“working team”). They should conduct a short kick-off meeting in which the LSA informs the CSAs about the very basic facts of the case and what it has done so far. It may be helpful to provide a summary of the most important facts of the case that are available<sup>10</sup> to facilitate a first exchange of thoughts by the working team. Ideally, the kick-off meeting shall take place very shortly after the plenary meeting in which the case was designated, or, if appropriate, even before that plenary meeting.

### 2.2. Making an action plan / Second Meeting / MoU

As a next step, the Action Plan should be established, ideally within four weeks after the plenary has designated the case as strategic. The Action Plan should at least include the following elements:

- The LSA and the dedicated CSAs should explain their self-set means of the prioritisation of the case.
- The LSA and the dedicated CSAs should define the tasks and roles within the working team, in particular of the CSAs. From the outset, the CSAs’ role is rather reactive, i.e. they receive information by the LSA and provide constructive feedback. Depending on the case, CSAs could also take a more active role, e.g. proactively sharing own existing information about similar cases, carrying out legal research on specific questions, or collect factual information within their own territory. The EDPB notes that, where it is envisaged that the CSAs shall take investigatory measures within the meaning of Article 58(1) GDPR, the cooperation is elevated to a “joint investigation” and the legal

---

<sup>10</sup> The “summary of key issues” as contained in the procedural regulation could serve as an orientation.

requirements of Article 62 become fully applicable. In such case, a more detailed Action Plan may be required.

- The working team shall jointly agree on a timeline in order to “ensure that the work will be conducted in the most efficient manner”<sup>11</sup>. The working team should be free to decide on the format of the Action Plan and may include, where appropriate, other elements, such as:
  - means of communication (e.g. not exclusively IMI but also informal formats such as e-mail, phone or video calls, in-person meetings, etc.);
  - frequency of internal communication;
  - external communication (i.e. how to possibly inform the public about the ongoing investigation);
  - “early adoption” by the SAs on a voluntary basis of elements for reaching consensus under the procedural regulation such as “summary of key issues” or “preliminary findings”;
  - implementation of the right to be heard.

### 2.3. Facing challenges

If the working team cannot agree on an action plan or for whatever reason the action plan cannot be followed, the working team should try to resolve those issues swiftly in the spirit of the principles laid out in this guide. The SAs should follow a layered approach. First and foremost, the dialogue between the LSA and the CSAs shall be intensified in order to avoid unnecessary escalations. If necessary, the LSAs and the CSAs should seek the advice of another SA that acts as a mediator. The SAs should report the results of their dialogue to the ENF ESG.

### 3. Reaching Consensus and internal communication

The Guidelines 02/2022 on the application of Article 60 GDPR clarify<sup>12</sup> that the SAs should use all possible tools, including mutual exchanges of relevant information, providing each other with an opportunity to express their views on exchanged information and take into account the point of view of other CSAs in order to reach consensus. This is particularly important in cases of strategic importance.

For the exchange of such information, not only the IMI system should be used. In addition, the LSA should offer to explain important results of the investigation by email or in videoconferences. The exchange in such videoconferences might be also helpful in order to ensure that the SAs work together, not against each other in the cooperation procedure. The LSA should make use of the possibilities of Article 60(2) GDPR in a collegial manner if it deems necessary or appropriate for the case at hand.

---

<sup>11</sup> See Vienna statement, page 1, point b).

<sup>12</sup> See Paragraph 42 of the Guidelines.

In line with the principles of transparency and collegiality, the LSA and the CSAs should report regularly report a state of play of the investigation to the ENF ESG. In particular, the members of the ENF ESG should be informed especially if adjustments of the timeline are necessary. The reporting should be kept simple and informal. The members of the ENF ESG should get the opportunity to briefly discuss the report. The working team may seek the views of the members of the ENF ESG on specific points in more detail, where it deems this helpful. In addition, important results and milestones should be reported to the Plenary. The extent of the information, which is presented to the Plenary must be decided on a case-by-case basis. In case of disagreements on important legal questions that are decisive for the outcome of the case, the working team may consult the ENF ESG, and if need be, the EDPB plenary for non-binding orientation. The working team should seek to anticipate potential RROs and to avoid them by finding early consensus. However, if it is clear that disagreements persist, the working team may also, in a spirit of collegiality, “agree to disagree” and communicate this in a transparent manner to the ENF ESG.

#### 4. External Communication

The working team may agree upon a communication strategy in the action plan, taking due account of the applicable law and potential risks for the integrity of the investigation identified by the LSA. In the first place, it is up to the LSA to decide whether to communicate the results of the investigation, for instance via press release or the publication of the final decision. Therefore, external communications, up until the date on which the final decision has been published by the LSA, may take place only with the agreement of the LSA. In addition, the final decision should in principle be published on the EDPB’s website if that is permitted by the national law of the LSA. In principle, the communication should indicate that the final decision was based on procedure that had been designated as a strategic case by the EDPB, unless the plenary decides otherwise. The withdrawal of a case should be communicated if the designation as a strategic case had already been announced in public.

## III. CLOSING OF A STRATEGIC CASE

This last section aims to list some situations in which a strategic case could be considered as closed.

#### 1. Submission of the Draft Decision in IMI by the LSA

In principle, the enhanced cooperation on a strategic case is completed as soon as the LSA has submitted the draft decision.

If, despite the enhanced cooperation, a CSA expresses a relevant and reasoned objection to the draft decision, the working team shall support the LSA’s assessment whether the relevant and reasoned objection should be followed.

After the final decision has been issued the LSA should inform the Plenary. The EDPB should publish the results of the case in a press release.

## 2. Withdraw of the strategic case by the EDPB Plenary

In certain circumstances, the strategic case could close naturally because it no longer meets the relevant strategic criteria. The selection of a case as a strategic case can take place at a very early stage, in particular before the end of the investigations carried out by the LSA. Depending on the elements revealed during the investigation, the case, although considered by the Plenary a strategic case, may turn out to be of lesser importance, or even lose its character as a cross-border case.

When the working team realizes that the strategic case no longer meets one of the selection criteria or that the reasons given at the time of its selection no longer exist, the LSA in consultation with the authorities of the working team proposes to downgrade this case by following the same procedure as that for selecting a case as a strategic case, namely a discussion within the ENF subgroup, then submission to the Plenary of the downgrading of the case from the list of strategic cases.

## TEMPLATE

### Proposal for cooperation on strategic cases

Applicant SA (insert the name of your SA)

#### A. Background information

1. **Data controller/processor's name:**
2. **LSA:**
3. **CSAs:**
4. **IMI number (if any):**

#### B. Summary of the case

1. **Facts and current status** (i.e. investigations already led by the applicant, key dates, number of complaints, of data subjects, etc.):
2. **Legal References** (e.g. Transparency (Article 12), Right of access (Article 15), etc.):
3. **Subject Matter** (e.g. Biometric data, Health care, etc.):
4. **Key Findings** (max 150 words):

#### C. Why does this case qualify as a strategic case?

- It concerns a structural or recurring problem in several Member States  
Which one?

- Case related to the intersection of data protection with other legal fields  
Explain briefly:
- A large number of data subjects in several Member States are affected by the processing operation  
How many?
- A large number of complaints have been received by your DPA  
How many?
- A fundamental issue falling within the scope of the EDPB strategy
- Case where the GDPR implies that a high risk can be assumed (processing of special categories of data as referred to in Articles 9 and 10 of the GDPR; processing regarding vulnerable people such as minors; or situations mentioned in Article 35 (3) of the GDPR where a data protection impact assessment (DPIA) is required, or situations where a DPIA is required based on the criteria for processing operations that are likely to result in a high risk as laid down in the Guidelines on Data Protection Impact Assessment.  
Explain briefly:

#### D. What is the added value of this cooperation and what kind of help do you expect/offer?

For instance: what kind of expertise is required, is there a proposed timeframe, how much support / capacity do you expect is needed, will you ask assistance from the pool of experts)

## TEMPLATE Action Plan

- **Background, objective, and scope of the investigation**

- **Participating SAs in the working team**

**LSA:**

**CSAs:**

- **Tasks of the members of the working teams**

Who	What	When

- **Dates (or milestone) of the investigation**

**Kick off Meeting of the working team:**

**Status meetings:**

**Granting of the right to be heard:**

**Presentation of the preliminary draft decision:**

**Upload of the draft decision in IMI:**

- **Means of internal Communication and reporting**
- **External Communication**
- **Contact details of the members of the working team**



European Data Protection Board

**Anu Talus**

Chair of the European Data Protection Board

Adrian Lobsiger  
Federal Data Protection and Information Commissioner

Copied to: John Edwards  
UK Information Commissioner

Brussels, 16 July 2024

*by e-mail only*

***Subject: Response to Letter on “Meeting on International Cooperation Launched by the ICO in Washington DC”***

Dear Commissioner Lobsiger,

Thank you very much for your letter dated 8 May 2024, as well as for your letter of 7 June replying to Commissioner Edwards' letter of 5 June to which I was copied.

First and foremost, I appreciate the input you shared with regard to the European Commission and ICO's initiatives on international cooperation and your suggestions on the way forward, with the contribution of the EDPB. I would like to thank you as well for your expressed willingness to continue exploring routes of collaboration with the EDPB on matters of mutual interest.

Contributing to the global dialogue on data protection, including on data transfers, is a strategic priority for the EDPB. In particular, the EDPB and its members will continue to engage with the international community, promoting high data protection standards and reinforcing the EDPB's involvement in international discussions. The EDPB equally intends to further facilitate and strengthen cooperation between the members of the EDPB and non-EU countries' data protection and privacy authorities. In this context, we will increase our efforts relating to our contributions on international cooperation and supporting enforcement, and further develop our current approaches.

In that perspective, the EDPB welcomes the initiative launched by the European Commission and the goal of strengthening cooperation with all countries that benefit from an EU adequacy decision and ensuring safe data flows. While cooperation and exchanges take place in various existing international fora, the network of adequate countries brings together jurisdictions that took significant steps towards convergence and that share common values and objectives of ensuring a high level of protection of personal data. In this regard, I would also like to reassure you that the EDPB shares your views on the importance of avoiding duplication of efforts with regard to existing cooperation initiatives.

European Data Protection Board

Rue Wiertz, 60  
1047 Brussels



European Data Protection Board

Therefore, we will continue to exchange with the European Commission during the implementation of this initiative, to facilitate and support the cooperation of data protection authorities. The EDPB also takes note of the first ideas for concrete cooperation projects you mentioned as well as of the specific follow-up actions identified during the technical follow-up meeting organised by the European Commission on 30 May 2024.

Finally, I would like to inform you that the EDPB is planning to contact DPAs from countries with adequacy decisions to set up a meeting in the autumn. This meeting would run alongside an EDPB plenary meeting and provide the opportunity to further discuss the expected benefits, focus and form of our cooperation.

I am looking forward to continuing to collaborate and exchange our views.

Yours sincerely,

Anu Talus

**Anu Talus**  
Chair of the European Data Protection Board

European Union Agency for Cybersecurity  
Agamemnonos 14,  
Chalandri 151231,  
Greece

Brussels, 16 July 2024

*by email only*

***Subject: EU cybersecurity certification scheme on cloud services supporting compliance to GDPR and cooperation options regarding the eHealth sector - EDPB reply letter***

In your letter of 11 March 2022, you had proposed to work together “to draw up, for instance, common cybersecurity requirements related to data protection into a dedicated extension profile, and guidance relative to data protection for both CSPs and cloud customers”. As a follow up, between September 2022 and January 2024, ENISA representatives participated in EDPB experts’ subgroup meetings to discuss the matter, and they responded to a questionnaire sent by the EDPB. I would like to thank you for this fruitful collaboration.

The EDPB finds that several important issues related to the links between the cybersecurity risk assessment in the European Cybersecurity Certification Scheme for Cloud Services (EUCS) and personal data protection risk assessment need to be addressed. Although the EUCS necessitates compliance with the law, it is not clear how, for example, the assurance levels of EUCS scheme may be mapped with usage scenarios involving personal data - which in turn poses questions on whether adoption of cybersecurity certification suffices to ensure appropriate security measures for a certification pursuant to the art. 42 of the GPDR.

The EDPB suggests to work together with ENISA by establishing a joint ad-hoc working group with the task to explore and assess the following possible objectives:

- Draw up guidance relative to data protection for both CSPs and cloud customers (e.g. map the assurance levels of EUCS scheme with usage scenarios involving personal data, or clarify that some of them can be flagged as generally non-sufficient for the processing of personal data).
- Assist DPAs, GDPR Certification scheme owners, or GDPR Codes of Conduct owners to articulate GDPR tools (certification, code of conduct, etc.) with the EUCS scheme



European Data Protection Board

- Develop a risk assessment methodology in order to assess the circumstances in which the EUCS assurance levels escalate along with the data protection risks, and to check whether the security measures envisaged in each of the EUCS assurance levels mitigate (and to what extent) the associated data protection risks
- Create an EUCS dedicated extension profile covering GDPR related additional requirements

We are therefore open to discuss and explore with you the appropriate shape and form of this collaboration.

Yours sincerely,

Anu Talus



European Data Protection Board

**Anu Talus**

Chair of the European Data Protection Board

Mr Michael McGrath  
European Commissioner for Justice

Brussels, 5 December 2024

*Via Ares*

**Subject: EDPB letter to the European Commission on its review of its eleven adequacy decisions adopted under Directive 95/46/EC**

Dear Commissioner McGrath,

On 15 January 2024, the European Commission concluded its review of eleven existing adequacy decisions adopted on the basis of Article 25(6) of Directive 95/46/EC which remained in force by virtue of Article 45(9) of the GDPR. In its report<sup>1</sup>, the Commission found that personal data transferred from the European Union<sup>2</sup> to Andorra, Argentina, Canada, Faroe Islands, Guernsey, the Isle of Man, Israel, Jersey, New Zealand, Switzerland, and Uruguay continues to benefit from adequate data protection safeguards. As a result, personal data transfers from the Union to these countries or territories can take place without additional requirements.

In its report, the Commission considered the data protection frameworks in the aforementioned eleven countries and territories, including the rules governing access to personal data by public authorities, in particular for law enforcement and national security purposes. The report is accompanied by a Staff Working Document (SWD)<sup>3</sup>, which presents the detailed findings of the Commission that lead to the conclusion that each of the eleven countries and territories continues to ensure an adequate level of protection for the personal data transferred from the Union.

The EDPB acknowledges the extensive work carried out by the Commission in reviewing the legislation and practices of the eleven countries and territories involved and notes that the draft report, together with the SWD, provides transparency with regards to the Commission's assessment. The EDPB also welcomes the fact that, according to the Commission's report, many countries and territories have

---

<sup>1</sup> [Report](#) from the Commission to the European Parliament and the Council on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC.

<sup>2</sup> Following its incorporation in the European Economic Area (EEA) Agreement, the GDPR also applies to Norway, Iceland and Liechtenstein. References to the EU in this letter are to be understood to also cover the EEA States.

<sup>3</sup> [Commission Staff Working Document](#) - Country reports on the functioning of the adequacy decisions adopted under Directive 95/46/EC.

strengthened their data protection frameworks<sup>4</sup>. This has led to further convergence with the EU legal framework.

As no adequacy decision was repealed, amended or suspended by the Commission, the EDPB did not provide an opinion as per Article 70(1)(s) of the GDPR, neither for the part related to the data protection framework nor for the part related to access to personal data by public authorities, which was assessed for the first time. **Nonetheless, given the EDPB's involvement in previous reviews of adequacy decisions<sup>5</sup> and its experience in this field<sup>6</sup>, the EDPB, while not questioning the substance of the report, would like to provide the Commission with observations on the methodology of its adequacy assessment and certain aspects that could have been described in more detail in the report and the SWD. The EDPB believes these aspects deserve close monitoring by the Commission in its future re-evaluations of third countries and territories' laws and practices under Article 45(4) GDPR and Article 97(2)(a) GDPR.**

## I. General remark

In line with Article 45(2)(a) and Recital 104 of the GDPR, the Commission's assessment of a third country takes into account how a particular third country respects the rule of law, access to justice as well as international human rights norms and standards. In light of this and in view of current developments, the EDPB would like to seize this opportunity to invite the Commission to provide more transparent information on the assessment of these elements, in law and in practice, in the context of future adequacy decisions and reviews.

## II. Observations on the methodology of the assessment of the data protection framework

When carrying out the adequacy reviews, according to Article 45(4) GDPR, the European Commission shall focus on the relevant developments in the legal frameworks of the third country or international organisation. The EDPB notes that accordingly, the January 2024 report and its SWD related to the eleven adequate third countries and territories did not provide a full description of the laws and practices of each third country or territory.

---

<sup>4</sup> [Report](#) from the Commission to the European Parliament and the Council on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC, pages 5-6.

<sup>5</sup> See, in this regard, the EDPB considerations included in the [Adequacy Referential](#) (issued by the Article 29 Working Party and adopted on 28 November 2017, WP 254) according to which, in order to allow the EDPB to provide the European Commission with an opinion on whether the third country, a territory or one or more specified sectors in this third country or an international organization, no longer ensures an adequate level of protection, the EDPB should be kept informed of any review process and review mission in the third country or to the international organization and would also appreciate to be invited to participate in these review processes and missions. See also, on this, Article 97(4) and Recital 106 GDPR according to which, for the purposes of carrying out the periodic reviews of the adequacy decisions envisaged by Article 97(2)(a) GDPR, the Commission should take into consideration, along with the views and findings of the European Parliament and of the Council, also the views of other relevant bodies.

<sup>6</sup> Article 29 Working Party (Art. 29 WP) had issued opinions on each one of the adequacy decisions adopted under Directive 95/46/EC at the time of their adoption. They can be found [here](#).

However, these adequacy decisions were adopted several years ago<sup>7</sup> and the elements to be taken into account in an adequacy assessment have evolved since the adoption of the original adequacy decisions<sup>8</sup>. **Against this background, the EDPB would have found it useful if this report contained a more comprehensive description of the elements of the adequacy assessment for each country and territory. The EDPB would also suggest, for future reports on the re-evaluation of the data protection frameworks related to these eleven adequate third countries and territories, that they contain a detailed description of the elements of the adequacy assessment for each country and territory or at least include references to previous reports or adequacy decisions where those elements are referred to.**

In this perspective, the EDPB considers that such future adequacy review reports could state more clearly which aspects of the third country laws and practices have been checked and have remained unchanged (and are not described in the report for this reason), as well as which aspects have evolved since the adoption of the initial decisions. This would provide a more comprehensive overview on the data protection guarantees existing in the assessed jurisdictions and might contribute to positive developments of the legal framework in other third countries. Additionally, it would provide data subjects with more transparency and enhance their understanding with regards to exercising their rights in the third country.

In particular, in this regard, the EDPB would like to draw the Commission's attention to the following aspects that are not mentioned consistently in the reports of *all* eleven countries and territories.

**The EDPB would therefore suggest describing in more detail in their future adequacy reviews for these eleven countries and territories:**

- i. **the legal notions of “controller”, “processor” and “recipient” or of equivalent notions<sup>9</sup>;** Although these data protection concepts do not have to mirror the GDPR terminology, they should reflect and be consistent with the concepts enshrined in European data protection law<sup>10</sup>;
- ii. **the legal bases under which personal data may be lawfully, fairly and legitimately processed;** The Union framework acknowledges several legitimate grounds for data processing including, but not limited to, performance of a contract or the legitimate interests of the controller or a third party which do not override the interests of the individual<sup>11</sup>; The

---

<sup>7</sup> The decisions on New Zealand and Uruguay were adopted in 2012, that of Canada was adopted in 2001 and that of Switzerland was adopted in 2000.

<sup>8</sup> See Judgment of the Court of Justice of the EU of 6 October 2015 in Case C-362/14, Maximillian Schrems v Data Protection Commissioner ([Schrems I](#)), ECLI:EU:C:2015:650; Judgment of the Court of Justice of the EU of 16 July 2020 in Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd. and Maximilian Schrems ([Schrems II](#)), ECLI:EU:C:2020:559. ; See Adequacy Referential.

<sup>9</sup> This issue is not expressly described in the reports of Andorra, Canada, Israel and New Zealand. It is on the contrary mentioned in the cases of Argentina, Faroe Islands, Guernsey, Isle of Man, Jersey, Switzerland and Uruguay, where such definitions exist.

<sup>10</sup> EDPB [Opinion 28/2018](#), §63-66; [Opinion 32/2021](#), §45 and 54; [Opinion 5/2023](#), §40.

<sup>11</sup> Opinion 32/2021, §63.

EDPB considers that the existence of legal grounds other than consent<sup>12</sup> (since consent has been sufficiently outlined in the reports) should be described in more detail in future assessments.

- iii. **the fact that individuals in the EU can exercise their rights in the third countries and territories**, as this would provide more transparency especially vis-à-vis data subjects;
- iv. **the inclusion of general descriptions and reassurances on limitations applicable to data subjects' rights<sup>13</sup> and not only in the context of access to the transferred data by third country authorities**; In this regard, the EDPB recalls that restrictions to data subject's rights should respect the essence of the fundamental rights and freedoms, and should be necessary and proportionate in a democratic society<sup>14</sup>;
- v. **the safeguards related to automated decision-making<sup>15</sup>, 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<sup>16</sup>, which the EDPB considers particularly important against the backdrop of the exponential development of AI technologies<sup>17</sup>.**
- vi. **the international commitments the third country has entered into<sup>18</sup> 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**. Adherence to international human rights commitments, to binding and non-binding international commitments are an indication of the respect of fundamental rights of individuals, including the right to the protection of personal data<sup>19</sup>;
- vii. **the rules on onward transfers** in the assessed third countries and how their application in practice<sup>20</sup> has developed since the adoption of the adequacy decisions. The EDPB notes in this regard that the applicable legal frameworks - in particular, in what concerns the transfer mechanisms available – appear to be, in some cases, very different from the ones set out under EU law, and recalls that the level of protection of individuals whose personal data is

---

<sup>12</sup> This issue is not mentioned in the reports of Jersey, Israel and Uruguay. It is on the contrary mentioned in the cases of Andorra, Argentina Canada, Faroe Islands, Ile of Man, New Zealand (partially) and Switzerland.

<sup>13</sup> This aspect is not mentioned in the reports of Argentina, Canada, Israel and Uruguay. It is on the contrary mentioned in the cases of Andorra, Faroe Islands, Guernsey, Isle of Man, Jersey, New Zealand, Switzerland.

<sup>14</sup> See Adequacy Referential, Chapter 2.A.8; See also Opinion 28/2018, §93 and 95.

<sup>15</sup> See Adequacy Referential, Chapter 3.B.3.

<sup>16</sup> This aspect is not mentioned in the reports of Argentina Canada, Israel and New Zealand. It is on the contrary mentioned in the cases of Andorra, Faroe Islands, Guernsey, Isle of Man, Jersey, Switzerland and Uruguay.

<sup>17</sup> See also Opinion 5/2023, §62-65.

<sup>18</sup> This aspect is not mentioned in the reports of Canada, Israel and New Zealand. It is on the contrary mentioned in the cases of Andorra, Argentina, Faroe Islands, Guernsey, Isle of Man, Jersey, Switzerland and Uruguay.

<sup>19</sup> See Recital 105 of the GDPR; Article 45(2)(c) GDPR; Adequacy Referential, Chapter 1 & Chapter 3.C.2 and 4; Opinion 32/2021, §34; Opinion 28/2018, §57; Opinion 5/2023, §22.

<sup>20</sup> For example, a description of the specific safeguards to be implemented by the exporter and their functioning, if possible with references to guidelines adopted by the competent data protection authority in this regard.

transferred to a third country must not be undermined by onward transfers to other third countries<sup>21</sup>.

### **III. Observations applying to the access to and use of personal data transferred from the EU by public authorities in the third countries.**

**Government access to personal data by third country public authorities** gained genuine significance for the question of whether a third country provides an adequate level of protection following the findings of the Court of Justice of the European Union (CJEU) in its *Schrems I* judgement<sup>22</sup>. The CJEU finds that data collection and processing by public authorities, in particular for law enforcement and national security purposes, is a key element of the adequacy standard<sup>23</sup>. The GDPR reflects this by explicitly referring in Article 45(2)(a) to legislation concerning public security, defence, national security, criminal law and the access of public authorities to personal data.

Against this background, government access to personal data has not been examined by the Commission in the procedure for adopting the eleven adequacy decisions now confirmed in its report, as the latter were still adopted under the former EU data protection framework and pre-date the CJEU's jurisprudence mentioned above. The EDPB therefore welcomes that the report of the Commission now **provides an assessment of the legal framework governing the access to and use of personal data transferred from the EU by public authorities of the third countries** that were found to provide an adequate level of protection pursuant to Article 25(6) of the Directive.

At the same time, the EDPB notes that the information provided in the SWD is not as detailed as in the context of a draft adequacy decision submitted to the EDPB for its opinion as per Article 70(1)(s) GDPR. In addition, as mentioned above, the EDPB was not formally consulted by the Commission since no adequacy decision was repealed, amended or suspended. It is therefore within these limits, and on the basis of the standard elaborated for surveillance measures framed as the "European Essential Guarantees"<sup>24</sup>, that the EDPB wishes to address its following observations on government access for law enforcement and national security purposes which require particular attention and monitoring in the future.

**National legal systems may provide for exemptions from the applicable data protection rules for law enforcement and national security purposes**, typically on grounds of prejudice to legitimate public interests and objectives, such as the prevention, detection or investigation of a crime. Exempted provisions may include, for example, rules relating to the general principles of data processing, data subject rights as well as oversight functions and powers. The EDPB would like to emphasise that such **exemptions and limitations need to be applied restrictively to ensure that they**

<sup>21</sup> Adequacy Referential, Chapter 3.A.9.

<sup>22</sup> See note 7 above.

<sup>23</sup> Ibid, §84 et seq. The Court clarified that the Commission's assessment should not be limited to the general data protection framework of the third country but should also include the legal framework for government access to personal data.

<sup>24</sup> [EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures](#), adopted on 10 November 2020.

**are only invoked to the extent necessary and proportionate in a democratic society.** It should not be possible to rely on exemptions from data protection standards in a blanket manner. In cases of exemptions on grounds of prejudice, competent authorities should be able to demonstrate that there is a real possibility of an adverse effect on the protected public interest *if* the relevant provision would be applied without restriction. Additionally, they should take into account the need for regular review of the circumstances justifying such limitations and for restoring their application where the justification for the limitations ceases to exist. **The EDPB invites the Commission to monitor the application of aforementioned exemptions in practice, in particular in jurisdictions where the law is broadly drafted and framed through interpretative but non-binding guidance issued by supervisory authorities. The Commission should follow up in future reports on the compliance with such guidance by governmental bodies.**

Following additional explanations provided by the Commission, the EDPB notes that the Commission has undertaken an **analysis of the impact of more general exceptions on the right to privacy and the protection of personal data for its reports (e.g. states of emergency)**. However, in particular from the point of view of access to personal data by public authorities, the EDPB would have appreciated if the Commission had included this analysis or at least its impact on the adequacy findings in the SWD, and thus made it publicly available.

Moreover, the EDPB encourages the Commission to draw up a more detailed overview of the intelligence landscape in the examined jurisdictions. The EDPB is aware that not all intelligence agencies in a given jurisdiction have access to personal data transferred or being transferred from the Union and that the methodology for drafting these reports depend on the information provided by the states under review. **The EDPB believes that such an overview would strengthen the data subjects' understanding of the rights and the remedies available to them and, thereby, put them in a better position to exercise their rights.**

Particularly in the area of government access for law enforcement and national security purposes, **oversight processes are likely to be multi-layered, involving several oversight structures, with differing powers.** For example, supervisory authorities may have extensive investigatory powers, but may not have binding remedial powers. In light of this, the EDPB invites the Commission to closely monitor to avoid that there is a gap between responsibilities and competences allocated to different oversight bodies in national systems. The EDPB encourages the Commission to ensure that **supervisory authorities collectively have adequate enforcement powers to ensure compliance with data protection laws.**

Another area for particular attention is represented by the **national provisions allowing, under certain conditions, business organisations or public sector bodies to disclose personal information on a voluntary basis** (i.e. upon informal requests from law enforcement authorities and intelligence



European Data Protection Board

agencies or on their own initiative). In this regard, it is essential that appropriate safeguards are envisaged to protect the rights and interests of the concerned individuals against arbitrariness<sup>25</sup>.

Moreover, with regard to ex-post reviews, the obligation to keep record of voluntary disclosures is essential since it allows oversight bodies to conduct full reviews of the use of these measures (e.g. with regard to the decision to disclose and the reasons to disclose as well as the information disclosed). **Therefore, the EDPB invites the Commission to closely monitor the national provisions allowing law enforcement authorities and intelligence agencies to obtain personal data transferred under the adequacy decisions through voluntary disclosures and their application in practice as well as the developments in the relevant legal framework.**

The EDPB stands ready to be involved in the next periodic review of the eleven adequacy decisions adopted under the Directive 95/46/EC, as the EDPB does for all the periodic reviews of adequacy decisions adopted under the GDPR.

Yours sincerely,

Anu Talus

Cc : Ms. Ana Gallego Torres, Director-General (DG JUST)

---

<sup>25</sup> Such as an effective prior assessment or ex-post review by independent oversight bodies regarding the legality, necessity and proportionality of informal requests or proactive decisions to disclose, the adoption of adequate measures to mitigate the impact on the fundamental rights and freedoms of data subjects, as well as the obligation to consider the reasonable expectations of the concerned individuals and the adoption of less intrusive means to access personal information.



European Data Protection Board

**Anu Talus**

Chair of the European Data Protection Board

[REDACTED]  
[REDACTED]  
Ligue des Droits Humains  
Boulevard Léopold II, 53  
1080 Bruxelles  
Belgique

Brussels, 17 December 2024

*by e-mail only*

**Subject: EDPB Reply to the open letter to the EDPB on the United Nations Convention against Cybercrime**

Dear [REDACTED]

I would like to thank you for your email dated 27 September 2024, in which you enclosed the open letter to the European Data Protection Board (EDPB) on the United Nations Convention against Cybercrime. I sincerely apologise for the delay in our response, which was due to a technical issue. As a result, we were only recently made aware of your communication.

With regard to the concerns raised in the open letter, I wish to draw your attention to the fact that the EDPB has recently issued a [Statement on the recommendations of the High-Level Group on Access to Data for Effective Law Enforcement](#). As this statement directly addresses the issues you have highlighted, we would refer you to this document for further information on the position of the EDPB on the matter. Please see in particular section 3, which addresses data security and encryption.

While, at this stage, the EDPB does not intend to issue a specific statement on the United Nations Convention against Cybercrime, the EDPB will continue to follow the matter very closely.

Yours sincerely

Anu Talus



European Data Protection Board

**Anu Talus**

Chair of the European Data Protection Board

Ms. Roberta Metsola, President of the European Parliament  
Mr. Javier Zarzalejos, Chair, Committee on Civil Liberties, Justice and Home Affairs (LIBE)  
Ms. Agnieszka Bartol, Permanent Representative of Poland to the European Union  
Ms. Thérèse Blanchet, Secretary General Council of the European Union  
Ms. Ursula von der Leyen, President of the European Commission  
Mr. Michael McGrath, Commissioner for Democracy, Justice and the Rule of Law

Brussels, 10 March 2025

Dear Madam President, Dear Mr. Chair,  
Dear Madam Secretary of State, Dear Secretary-General,  
Dear Madam President, Dear Commissioner,

The draft regulation laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679 (“Draft Regulation”) is currently being discussed during trilogue meetings.

The EDPB strongly supports the objective of the Draft Regulation to streamline GDPR enforcement through faster, smoother and more efficient enforcement procedures.<sup>1</sup>

Considering the importance of the matter for the enforcement of the GDPR, for the effective cooperation between data protection authorities, and for the EDPB, I would like to express the full availability of the Board to support the ongoing work. The EDPB kindly requests that you keep us informed about the progress made on this valuable work and is available to participate in any technical meetings or provide any other contributions that may help with this ongoing process.

Yours sincerely,

Anu Talus

Copy:

Ms. Alina Gabriela Vasile-Tovornik, Head of Unit of the LIBE Secretariat, European Parliament  
Mr. Serge de Biolley, Director JAI.2, General Secretariat of the Council of the European Union  
Ms. Ana Gallego, Director-General, DG JUST, European Commission  
Mr. Olivier Micol, Head of Unit C.3 - Data protection, DG JUST, European Commission

---

<sup>1</sup> EDPB-EDPS Joint Opinion 01/2023 on the Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679.

# Letters



Mr Didier Reynders  
European Commissioner for Justice

***Sent by e-mail only***

Brussels, 22 February 2022  
Ref: OUT2022-0009

Dear Commissioner Reynders,

The EDPB very much welcomes the Commission's initiative aiming at adapting liability rules to the digital age and artificial intelligence (AI) and wishes, in this context, to underline some elements that should be considered and could usefully complement the recent public consultation undertaken on this matter.

Building upon the 2018 evaluation of the Product Liability Directive and its main conclusions, the EDPB considers that the revision of this legal framework should ensure consistency with and complement the EU acquis in the field of personal data protection, in particular when it comes to the security of personal data processing and the use of AI systems to comply with this obligation.

While, under the GDPR, only controllers and processors would be liable, e.g., in case of a personal data breach, it is essential to consider the role and potential liability of providers of AI systems developed and made available in order to secure personal data processing. In such case, the EDPB considers relevant to strengthen the liability regime of providers of such AI systems, and ensure that processors and controllers can trustfully rely on those systems.

In their joint opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (the AI Act)<sup>1</sup>, the EDPB and the EDPS laid down a list of acknowledgements and recommendations. In accordance with this opinion, the EDPB wishes to reiterate some of its recommendations and to underline some points of interest that should be considered when adapting the Product Liability Directive to the new challenges of AI systems.

---

<sup>1</sup> 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, available at: [https://edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-52021-proposal\\_en](https://edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en)

Firstly, the EDPB wishes to renew a recommendation regarding the clarity of role attribution that was already raised in the joint opinion 5/2021, and that gains further weight with the possible introduction of new attributions under the Product Liability Directive. In order to promote an efficient liability framework for AI systems that are used as security measures for personal data processing, the EDPB wishes to emphasize the importance of the interplay with existing regulation, such as the GDPR, especially when it comes to the attribution of responsibilities. So as to ensure clarity regarding this category of systems, the EDPB considers that the role and responsibilities of the provider of the AI system must be precisely defined to bridge the gap with the existing framework binding data controllers and data processors.

Secondly, the EDPB wishes to draw the Commission's attention to the importance of several aspects of AI that were underlined in the joint opinion 5/2021. Because of the nature of AI, assigning the responsibility to a party in a claim that involves an AI system might be particularly difficult, especially when the burden of proof lies with the individual since the latter could be unaware of the fact that AI is used and, in the majority of cases, would lack the necessary information to prove the liability of the AI system. Hence, the explainability of the system must be foreseen at the step of its conception so that the results of all intended use, foreseeable use and foreseeable misuse that could lead to a potential claim, will be explainable by design. For that purpose, the EDPB wishes to stress the positive effects of including systematic human supervision and transparency for the end user on the use and operation of the AI system and on the deployed methods and algorithms. Limitations and risks on the use of AI systems due to different types of attacks, e.g., cyber-attacks and adversarial attacks, should also be taken into consideration in the responsibility and liability schemes. Providers of AI systems should be responsible for providing users with mitigation tools for known and new types of attacks and for embedding security by design throughout the entire lifecycle of the AI, whereas users of AI systems should be responsible for ensuring the safe operation of the system. The EDPB considers that these measures should be mandatory, in particular when the AI system is used as a security measure for personal data processing but does not process personal data itself. Moreover, the AI system should be accompanied with a thorough and accessible documentation, as this piece of information would be necessary for the data controller to understand the cause of a system failure, especially if it led to a data breach, and to be able to stop the failure in a timely manner. Finally, the EDPB invites the Commission to ensure that the revised directive will allow any affected person to find effective legal remedies after a system failure or a successful attack.

Thirdly, specific liabilities might be triggered by the ineffective application of data protection principles by AI providers and users. Lack of data accuracy, or scarce attention paid to the fairness of algorithmic decisions might translate into impairments to individuals' rights and freedoms as well as damages or economic losses. It is essential that in the forthcoming legal regime on AI liability a primary role is vested by the preliminary assessment of the quality and representativeness of the data used by machine learning algorithms to draw their decisions. Measurability of the degree of fairness and causality of algorithmic decisions in general should be a pillar of the new liability rules in order to create a trustable technological environment and limit the negative effects arising from the occurrence of erroneous decisions.

Lastly, the EDPB wishes to underline that the proposal should be effective as a standalone legislation and not rely on the obligations laid by the AI Act. As was raised in the joint opinion 5/2021, the obligations laid on AI systems users and providers only apply to restricted categories of high-risk AI systems, whereas it is foreseeable that some AI systems that were not included in these categories could lead to possible claims and thus require a liability framework. While the GDPR and the future AI Act should be consistent with one another, the EDPB wishes to draw the Commission's attention on the possible legal void in which some AI systems could be left when they are neither considered high-risk under the AI Act, nor covered by the GDPR.

Yours sincerely,



Andrea Jelinek

# Letters



Henrik Hololei  
Director-General  
Directorate-General for Mobility and Transport  
European Commission

Brussels, 5 June 2019  
Ref: Ares(2019)1766235  
SH-941-2019

Dear Director-General Hololei,

I refer to your letter of 18 March 2019 in which you invite the European Data Protection Board members to issue a formal opinion on the Commission Delegated Regulation with regard to the provision of EU-wide Cooperative Intelligent Transport Systems, adopted on 13 March 2019.

As you noted, the Commission invited the Board members to express their views on the Draft Commission Delegated Regulation with regard to the provision of EU-wide Cooperative Intelligent Transport Systems in parallel with the inter-service consultation phase. An opportunity the Board appreciated, bearing in mind connected vehicles is part of the ongoing work program of the Board.

The Board refers to the comments previously provided, in accordance with article 70(1)(b) GDPR, on the draft delegated regulation's provisions and the revised wording of the now adopted delegated regulation, in particular with regard to data protection. The Board further takes note of the position expressed by the European Data Protection Supervisor regarding article 42(1) of Regulation 2018/1725 in this context. In light of the above, the Board will not be issuing a further opinion at this stage.

The Board points out that a number of essential issues remain unresolved in this context, in particular the clear identification of the data controllers involved in the C-ITS services, the necessity of conducting the Data Protection Impact Assessment and the application of the data protection by design and by default to the C-ITS services.

For the sake of clarity, the legal basis of processing, re-use of data for other purposes, privacy by default and by design, data minimization as well as security are among the topics the Board is looking into in its ongoing work on the topic of connected vehicles, taking into consideration the wider legal

framework and in particular to Directive 2010/40/EU. The Board will inform the Commission of any guidelines or recommendations it may issue on the subject of connected vehicles in future.

Finally, should the Commission wish to consult the European Data Protection Board in the future, potentially with regard to a future revision of Directive 2010/40/EU, do not hesitate to do so at an early stage of the process.

Yours sincerely,



Andrea Jelinek

Moritz Körner MEP  
European Parliament  
Rue Wiertz 60  
B-1047 Brussels  
Belgium

28 August 2020

Ref: OUT2020-0101

Dear Mr Körner,

I refer to your letter dated 23 January 2020 outlining your concerns in relation to the use of Microsoft 365, Facebook and Instagram on school computers.

Many thanks for bringing this important topic to our attention. Information on this matter has been forwarded to the national supervisory authorities for their consideration.

However, the EDPB is not able to comment on the activities of specific controllers and processors. The role of the EDPB is to ensure the consistent application of the GDPR, whereas the competence to handle complaints and launch enforcements actions lies with the national supervisory authorities. We are confident that the GDPR and EDPB cooperation mechanisms will enable the national supervisory authorities to work together and ensure the uniform application of the GDPR in the EEA.

We encourage controllers in the public and private sector to carefully assess the risks arising from their processing activities and ensure compliance with the principles and obligations set out by the GDPR, including in terms of legal basis for processing and international transfers, especially when the processing of personal data relating to vulnerable data subjects is at stake.

Please note that the EDPB is not in a position to discuss or comment on pending procedures.

Yours sincerely,



Andrea Jelinek

Moritz Körner MEP  
European Parliament  
Rue Wiertz 60  
B-1047 Brussels  
Belgium

10 September 2020

Ref: OUT2020-0102

Dear Mr Körner,

I refer to your letter dated 24 January 2020 outlining your concerns in relation to the practice of applications sharing personal data with advertising networks and third party providers.

Thank you very much for bringing this study to our attention. The EDPB is aware of the importance of this topic and has recently issued Guidelines on the targeting of social media users, now open for public consultation.

Additionally, the topic of privacy in the adtech industry is examined within the relevant EDPB Expert Subgroups. The EDPB and its Expert Subgroups also serve as a useful forum for the national supervisory authorities to coordinate, cooperate and exchange experiences in ongoing cases.

Please note that the role of the EDPB is to ensure the consistent application of the GDPR, whereas the competence to handle complaints and launch enforcements actions lies with the national supervisory authorities. Therefore, the EDPB lacks the competence to initiate an investigation regarding any specific company.

Yours sincerely,



Andrea Jelinek

Ms. Birgit Sippel MEP  
European Parliament  
60, Rue Wiertz  
B-1047 Bruxelles  
Belgium

28 August 2020

Ref: OUT2020-0103

Dear Ms Sippel,

Thank you for your letter dated 08 May 2020 regarding the enforcement of the GDPR against public authorities. In the context of the Covid-19 crisis, this issue has gained importance.

The enforcement of the GDPR lies within the competence of the national supervisory authorities. The Board itself cannot carry out any enforcement activities against public authorities in the Member States.

According to Art. 70 GDPR the role of the EDPB is to ensure the consistent application of the GDPR. To this end, the tasks of the Board include monitoring and ensuring the correct application of this Regulation in the cases provided for in Articles 64 and 65 GDPR without prejudice to the tasks of national supervisory authorities, and promoting the cooperation and the effective bilateral and multilateral exchange of information and best practices between the supervisory authorities.

To fulfil these tasks the Board has inter alia established the Enforcement Expert Subgroup. Within this Expert Subgroup the representatives of the national supervisory authorities exchange regularly information on matters of the enforcement of the GDPR in the Member States.

In the context of the enforcement of the GDPR administrative fines and other corrective powers have to be distinguished. Art. 83(7) GDPR contains an opening clause which allows the Member States to lay down rules in national laws on whether and to what extent administrative fines may be imposed on public authorities and bodies. Some Member States exercised this opening clause and excluded the possibility to impose fines on public authorities and bodies in their national legislations. Therefore, not in all Member States public authorities can be sanctioned by administrative fines. In contrast, Article 58(2) GDPR does not provide an opening clause in terms of other corrective powers of supervisory authorities. Thus, to the extent known, corrective powers pursuant to Article 58(2) GDPR different from fines can be issued against public authorities in all Member States. This also applies to German data protection authorities with the limitation, however, that under the federal data

protection law and the national data protection law of the German Laender nearly all supervisory authorities are not entitled to enforce corrective powers towards ministries or other state authorities in the event these authorities do not comply with corrective measures.

So far, the exchange of information in the Enforcement Expert Subgroup has not shown a general lack of powers endowed to national supervisory authorities to effectively issue corrective powers pursuant to Article 58(2) GDPR. Constraints like in the concrete case to which you refer in your letter have not been reported by other Member States.

The EDPB will continue to monitor the enforcement of the GDPR in the Member States. Within the scope of its competence the Board will examine any question which arise in the context of the enforcement of the GDPR.

Yours sincerely,



Andrea Jelinek

# Letters



Mr Juan Fernando López Aguilar  
Chairman  
Committee on Civil Liberties, Justice and Home Affairs  
European Parliament

***Sent by email only***

Brussels, 22 February 2022  
Ref: OUT2022-0008

Dear Mr López Aguilar,

Thank you very much for your letter of 15 November 2021 on behalf of the Committee on Civil Liberties, Justice and Home Affairs (the Committee), in which you inform about the Committee's request for an EDPB opinion on the final draft of the Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence (the Protocol).

The EDPB welcomes your request and the opportunity to recall its views for the Committee. The EDPB had indeed already called on the European Commission and European Parliament, as well as on EU Member States and national parliaments, to ensure that the Protocol negotiations receive careful scrutiny in order to guarantee the full consistency of the envisaged Second Additional Protocol with the EU acquis, in particular in the field of personal data protection.

In this context, the EDPB had the occasion to provide and publish its observations and recommendations during the negotiating process of the Protocol, addressing its points of concern and attention in relation to the draft provisions published at the time, and in particular in its latest contribution (annexed to this letter) to the 6th round of consultations in May 2021 on the draft Protocol, which has been since then adopted by the Committee of Ministers of the Council of Europe on 17 November 2021.

In response to your Committee's request, the EDPB wishes to recall some of the aspects of earlier statements and in the light of the two Commission's Proposals for Council Decisions authorising Member States to sign and to ratify, in the interest of the European Union, the Protocol (the Proposals). The EDPB regrets to note that many of its recommendations to the negotiations on the draft of the Protocol, to a great extent, are not reflected in the final version of the text.

Additionally, the EDPB wishes to refer to the EDPS Opinion 1/2022 on the above-mentioned Proposals. The EDPB wishes to highlight and complement some of the crucial points identified by the EDPS. Furthermore, the EDPB encourages the Committee to consider and address the EDPS Opinion and its recommendations in its assessment of the Protocol.

#### *On the effect of the Protocol and the Proposals*

The Council of Europe Convention on Cybercrime (hereinafter Cybercrime Convention), as well as any of its additional protocols, are to be considered as a legally binding and enforceable international instrument. In this regard, the EDPB stresses that, in line with the CJEU case law, the “obligations imposed by an international agreement cannot have the effect of prejudicing the constitutional principles of the EC Treaty, which include the principle that all Community acts must respect fundamental rights, that respect constituting a condition of their lawfulness.”<sup>1</sup>

The EDPB reiterates that from the perspective of the European Union and its Member States the Protocol must be assessed in light of EU law and case law, in particular by considering the provisions on appropriate safeguards as referred to in Chapter V of Regulation (EU) No 2016/679 (GDPR) and Chapter V of Directive (EU) No 2016/680 (Law Enforcement Directive) and their interpretation by the Court of Justice of the European Union (CJEU) in light of the EU Charter.

In this context, the EDPB emphasizes that Article 44 of the GDPR lays down provisions to ensure that any transfer of personal data from EU Member States to third countries shall only take place if the level of protection guaranteed by the GDPR is not undermined. Where the transfer is conducted by a competent authority as defined in Article 2(1) Law Enforcement Directive, the equivalent is specified by Article 37 of that Directive. Given that the Protocol could have an effect on the application of these provisions of EU law in the context of transfers, the EDPB reiterates that several provisions of the Protocol, and in particular those under Chapter II, section 2 related to the direct cooperation with providers and entities in other Parties may, given the level of norm and legal effect of the Protocol, also have an effect on transfer and disclosure, as per Chapter V GDPR and in particular its Article 48. It is therefore essential that the level of protection resulting from the Protocol for the exchange of personal data with third countries is essentially equivalent to the level of protection provided by EU law.<sup>2</sup>

#### *On measures for enhanced cooperation*

The EDPB welcomes the proposals of the Commission for the Member States to make, in the interest of the Union, the declaration, notification and communication under Article 7(2)(b), (5)(a) and (e) of the Protocol. These proposals ensure that service providers in the Union may be requested the

---

<sup>1</sup> CJEU Judgment of 3 September 2008 in joined cases C-402/05 P and C-415/05, Yassin Abdullah Kadi and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities, ECLI:EU:C:2008:461, par. 285.

<sup>2</sup> See also EDPS Opinion, paragraph 32.

transfer of personal data only on the basis of orders issued, in the requesting third country Party to the Protocol, by, or under the supervision of, a prosecutor or other judicial authority, or under independent supervision and under the control of a competent authority within the requested Member State.<sup>3</sup>

The EDPB also notes positively the proposal that Member States make the declaration under Article 8(4) of the Protocol (on the co-operation between competent authorities to give effect to production orders of subscriber information and traffic data), so as to ensure that additional supporting information is required to give effect to orders under this provision.<sup>4</sup>

In order to ensure the involvement of independent authorities, the EDPB fully supports the EDPS recommendation<sup>5</sup> for Member States to designate, pursuant to Article 7(5)(e) of the Protocol, a judicial or other independent authority.

Certain data contained in the category of subscriber information within the meaning of the Cybercrime Convention, may be deemed under EU law as traffic data (e. g. dynamically allocated addresses in IPv4) and the access to such data may entail a serious interference with the fundamental rights of the data subject. The CJEU has held in its recent case-law<sup>6</sup> that, access of national authorities to retained traffic data may be justified only by the fight against serious crime, and subject to a prior review carried out either by a court or by an independent administrative body. Therefore, the EDPB recommends, in line with the EDPS Opinion,<sup>7</sup> that Member States, contrary to the proposal of the Commission, reserve the right not to apply Article 7 of the Protocol on disclosure of subscriber data by service providers directly to competent authorities of another country in relation to certain types of access numbers, pursuant to Article 7(9)(b).

Finally, in relation to measures for enhanced cooperation, the EDPB reiterates the essential nature of the dual criminality principle, which aims at providing an additional safeguard to ensure that a State cannot rely on the assistance of another to apply a criminal sanction which does not exist in the law of another. In this regard, while the EDPB notes the lack of explicit reference to dual criminality in the Protocol other than in Article 5(6), the EDPB understands that this permission is to be found where the Protocol allows parties to add conditions to or refuse the transfer under their domestic law.<sup>8</sup>

#### On the conditions and safeguards related to the protection of personal data

While taking note of the further clarifications provided in the Explanatory Report,<sup>9</sup> the EDPB regrets that the extent to which parties may add further conditions and safeguards to the transfer of personal

<sup>3</sup> See also EDPS Opinion, paragraphs 89 and 90.

<sup>4</sup> See also EDPS Opinion, paragraph 96.

<sup>5</sup> EDPS Opinion, paragraphs 91 and 92.

<sup>6</sup> C-511/18 - La Quadrature du Net and Others of 6 October 2020.

<sup>7</sup> EDPS Opinion, paragraphs 93-95.

<sup>8</sup> See also paragraph 69 of the Explanatory Report.

<sup>9</sup> Explanatory Report, Paragraph 230.

data and the extent to which they may not be added, if they are considered as generic data protection conditions pursuant to Article 14(2)(a), have not been made clearer.<sup>10</sup>

In relation to the application of the proportionality principle and in line with its previous contribution (page 6), while welcoming the direct reference to Article 15 of the Cybercrime Convention in the Protocol,<sup>11</sup> the EDPB regrets that the application and implementation of the principle of proportionality is not explicitly included in the text of Article 13, in order to ensure legal certainty and clarity, and to enshrine this principle for any processing of personal data resulting from the application of the Protocol.

The EDPB regrets that its proposal concerning the onward sharing within a party to establish a mechanism to inform the transferring party of an envisioned onward sharing and further processing has not been implemented.<sup>12</sup>

The reference to the Parties' domestic legal framework in Paragraph 11 of Article 14 of the Protocol, read in conjunction with paragraph 12(a)(i) of Article 14, implies that possible limitations and restrictions to transparency and notice are to be permitted under the domestic legal framework of the receiving Party. The EDPB acknowledges, in line with the EDPS Opinion, that paragraph 12(a)(i) of Article 14 of the Protocol imposes specific conditions for such laws, as it provides for the "*application of proportionate restrictions permitted under [the receiving Party's] domestic legal framework, needed, at the time of adjudication, to protect the rights and freedoms of others or important objectives of general public interest and that give due regard to the legitimate interests of the individual concerned*". The EDPB wishes to recall in this regard that the domestic legal framework of third country Parties to the Cybercrime Convention applicable to restrictions on transparency and notice may significantly diverge from the ones in the Union or Member States' law, thus possibly resulting in limitations that may not be considered as compatible with Union or Member States' law.

The EDPB also regrets that its recommendations in relation to the exercise of data subject rights have not been taken into account and in particular that the provision under paragraph 12(b) does not ensure that, as a general rule, information to individuals related to access shall be provided free of charge.

While welcoming the obligation under the Protocol that "[e]ach Party shall have in place effective judicial and non-judicial remedies to provide redress for violations of *this article*" (paragraph 13 of Article 14), the EDPB regrets that neither the text of the Protocol nor the explanatory report explicitly clarifies that such redresses are available under the jurisdiction of each Party to the Cybercrime Convention to any concerned data subjects, as per the EDPB recommendation made in its previous contribution (page 12). Such application is essential to ensure full compatibility with EU law and

---

<sup>10</sup> See also in this regard EDPS Opinion, paragraphs 46, 56-60, 75, 80, 81 and 86- 87.

<sup>11</sup> See also paragraph 218 of the Explanatory Report.

<sup>12</sup> See also EDPS Opinion, paragraph 61.

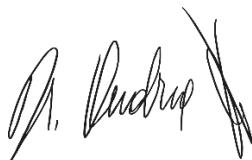
appears all the more important considering that not all Parties to the Cybercrime Convention fall under the jurisdiction of the European Court of Human Rights.

The EDPB welcomes the provisions on oversight and recommends (in line with the encouragement in the Explanatory Report<sup>13</sup>) establishing mechanisms to foresee the cooperation and exchange of information between established public authorities ensuring oversight in each Party, thus allowing for a coordinated and consistent supervision of the implementation of the Protocol and contributing to the assessment foreseen under its Article 23. In addition, the EDPB would like to emphasise that, in agreement with the EDPS Opinion, it considers that an eventual lack of an independent supervisory authority in another Party would constitute a systematic and serious breach within the meaning of paragraph 15, thus allowing transfers to be suspended to that Party.

In addition, with regard to the Council decisions, and in line with the EDPS Opinion,<sup>14</sup> the proposed communication by the Member States to the United States authorities, at the time of signature or when depositing their instrument of ratification, acceptance or approval, in relation to the EU-US Umbrella Agreement should be clarified.

The proposed consideration, in relation to other agreements or arrangements under Article 14(1)(c) of the Protocol that could replace the data protection provision of the Protocol (Article 14), should be amended in the Council's decisions, in line with the EDPS Opinion.<sup>15</sup>

Yours sincerely,



Andrea Jelinek

---

<sup>13</sup> Explanatory Report, paragraph 281. See also EDPS Opinion, paragraph 115.

<sup>14</sup> EDPS Opinion, paragraphs 121-122.

<sup>15</sup> EDPS Opinion, paragraphs 123-128.

# Letters



Brussels, 18 January 2022

Ref: OUT2022-0003

***Sent by e-mail only***

To whom it may concern

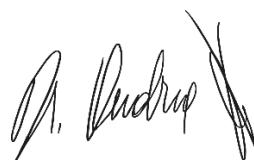
On July 23<sup>rd</sup> 2021, you addressed a letter to the EDPB calling for a consistent interpretation of cookie consent requirement by the EDPB to which the EDPB acknowledged receipt. On October 27<sup>th</sup>, 2021, you addressed a follow-up letter renewing your concerns.

First and foremost, I thank you for these two letters that I reviewed with great attention.

Please rest assured that the EDPB's aim is to ensure the harmonised application of data protection rules throughout the European Union. To this end, the Board promotes the consistent interpretation of consent requirements in the context of cookies among the data protection authorities. I also take the opportunity to assure you that neither the EDPB nor its members have any interest or intention to deviate from the text, spirit or intent of the e-privacy legal framework and the GDPR.

In this respect, and as you mentioned in your latest letter, the EDPB established a taskforce on cookie banners. Lastly, and as you are aware of, the EDPB guidelines on consent have been updated (by Guidelines 05/2020 on consent under Regulation 2016/679) in order to ensure a harmonized approach on to the conditionality of consent and on the unambiguous indication of wishes.

Yours sincerely,



Andrea Jelinek

**Andrea Jelinek**  
Chair of the European Data Protection Board

rue Wiertz, 60  
1047 Brussels

MEP Sophie In 't Veld  
[sophie.intveld@ep.europarl.eu](mailto:sophie.intveld@ep.europarl.eu)

**By e-mail only**

Brussels, 23 January 2019

**Ref:** SH-423-2018

**Subject: Letter from 12 November 2018 on Romanian DPA Investigation**

Dear Ms In 't Veld,

I would like to thank you for the letter you sent me on 12 November 2018 on the order issued on 9 November by the Romanian data protection authority to investigative journalists of the RISE project, to disclose their sources on the basis of the General Data Protection Regulation (GDPR).

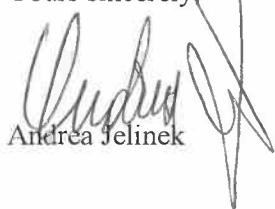
As foreseen in article 58 GDPR, each Supervisory Authority (SA) has the power to request any information from a controller or from a processor in the context of a given processing operation that is necessary for the performance of its tasks. The fundamental right to the protection of personal data that such power aims to protect, however, has to be balanced against the protection of other equally important fundamental rights (such as the right to freedom of expression and information). It goes without saying that the protection of journalistic sources is a cornerstone of the freedom of the press.

Furthermore, such powers must take into consideration the requirements foreseen in article 85 GDPR, which mandate a legal reconciliation of both fundamental rights, including in cases where processing for journalistic purposes is involved. Even though article 85 leaves such task to Member States, it is clear that such reconciliation must always be done in respect of chapter VII GDPR and of the applicable jurisprudence of the CJEU and the ECtHR.

Moreover, it is also essential to add that such powers should be exercised in a proportionate manner and based on an individual assessment of each case. The same reasoning is applicable to any fines issued by an SA under the GDPR: they need to be imposed casuistically and be, not only effective and dissuasive, but also proportionate to the demonstrated infringement.

I would like to underline that the European Data Protection Board (EDPB) does not have the same competences, tasks and powers as national supervisory authorities. The assessment of alleged infringements of the GDPR in first instance falls within the competence of the responsible and independent Supervisory Authorities of each Member State, either by themselves or in cooperation with other SAs. A judicial remedy will always be available in accordance with article 78(1) GDPR.

Yours sincerely

  
Andrea Jelinek

**Andrea Jelinek**  
Chair of the European Data Protection Board

rue Wiertz, 60  
1047 Brussels

MEP Sophie In 't Veld  
[sophie.intveld@ep.europarl.eu](mailto:sophie.intveld@ep.europarl.eu)

**By e-mail only**

Brussels, 23 January 2019

**Ref: SH-464-2018**

**Subject: Letter dated 23 November 2018 on Spanish electoral law**

Dear Mrs In 't Veld,

Thank you very much for your letter dated 23 November 2018 concerning the recently approved Spanish electoral law.

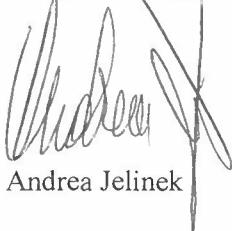
The processing of sensitive personal data, such as political opinions, in particular in an electoral context, is of great relevance to the European Data Protection Board and to all its members. Elections are a pillar of the democratic process and, given recent events, it is imperative to ensure a lawful processing of personal data in this context.

The GDPR, in its recital 56, determines that the processing of political opinions of data subjects by political parties is permitted for reasons of public interest where - and I underline the importance of this part - "appropriate safeguards are established".

For your information, the Spanish SA has adopted an opinion on this matter on the 19th December 2018.<sup>1</sup>

Separately, given the importance of the processing of personal data in an electoral context, I am in a position to inform you that the Board intends to produce a general statement on this subject.

Yours sincerely,



Andrea Jelinek

<sup>1</sup> See <https://www.aepd.es/media/informes/2018-0181-tratamiento-datos-opiniones-politicas-por-partidos-politicos.pdf>; you can find a summary through this link: <https://www.aepd.es/prensa/2018-12-19.html>.



To: The Presidency of the Council of the EU

Brussels, 9 October 2019

Ref: OUT2019-0035

**By email only**

Dear Madam or Sir,

The Article 29 Working Party adopted two Opinions in 2008 and 2009 (WP156 and WP 162) on certain relevant provisions of the World Anti-Doping Code and the International Standards completing the Code. In 2013, the Article 29 Working Party sent a letter to WADA (Ref. Ares (2013)289160 - 05/03/2013) with a number of observations and concerns with regards to the Code and its International Standards.

The European Data Protection Board (EDPB), as successor of the Art.29 Working Party, has attentively followed the activities of the World Anti-Doping Agency, and particularly the different phases in the revision process of both the World Anti-Doping Code and of the International Standards.

With this letter, in the context of the third and final stage of the public consultation organised by WADA, the EDPB firstly acknowledges that essential progress has been made in relation to the safeguards on privacy and data protection provided by the Code and its Standards and that a few of the Article 29 Working Party's remarks outlined in its earlier opinions and in its letter to WADA have been taken into account during the revision process of the anti-doping rules. Nevertheless, on the occasion of the third and final stage of the public consultation organised by WADA, we would like to raise some remaining concerns regarding these documents, particularly in respect of the latest modifications brought to them by WADA. These concerns mainly relate to aspects already highlighted in the previous contributions of the Art. 29 Working Party, such as the issue of the lawfulness of data processing based on consent, the application of the International Standard for the Protection of Privacy and Personal Information vis-à-vis the Code and/or the other applicable laws laying down rules setting a lower level of protection for privacy and personal data, as well as the retention periods and the automatic and unselective publication of anti-doping rule violations on the Internet.

The EDPB will not reiterate all the remarks mentioned in the earlier contributions of Article 29 Working Party already endorsed, but if they have not been considered in the different phases of the current revision process, they should be considered as having been restated with this letter. In addition, you will find further remarks on the compliance of the WADA Code and its International Standards with the General Data Protection Regulation (hereinafter GDPR) annexed to this letter.

The EDPB makes these observations in light of the level of protection offered by the GDPR, currently in force.

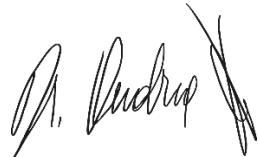
**Andrea Jelinek**  
Chair of the European Data Protection Board

rue Wiertz, 60  
1047 Brussels

The EDPB calls upon WADA to take into account its remarks, which are aimed at safeguarding a level of data protection equivalent to that of the EU, but also, more fundamentally, at promoting the highest possible level of data protection in the interest of all individuals concerned.

The EDPB remains at WADA's disposal for any further information or explanation regarding its observations.

Yours sincerely,



Andrea Jelinek



**Andrea Jelinek**  
Chair of the European Data Protection Board  
rue Wiertz, 60  
1047 Brussels

## Remarks and comments on the compliance of the WADA Code and its International Standards<sup>1</sup> with the GDPR<sup>2</sup>

Address the issue of Data Controller/Data processor (cf. Art. 29 WP's second Opinion 4/2009, 2.2)

As mentioned in the Second Opinion 4/2009 of the Art. 29 WP<sup>3</sup>, there is still no reference in the Code nor in the Standards concerning the issue of data controller/data processor for any particular processing. It could be of particular relevance to address this issue, especially regarding non-EU-bodies acting as data controller in the EU or non-EU-bodies collecting data of EU individuals.

Extending the scope to recreational-level Athletes is an interference (cf. Art. 29 WP's second Opinion 4/2009, 3.1)

With regard to the term "Athlete" which refers to any Person who competes in sport at the international or at the national level, the Code specifies that any Anti-Doping Organization (hereinafter ADO) has discretion to apply anti-doping rules to Athletes who are neither International-Level Athletes nor National-Level Athletes, and thus to bring them within the scope of the Code and of its International Standards. Thus, the definition allows each National ADO, if it chooses to do so, to expand its antidoping program beyond International- or National - Level Athletes to competitors at lower levels of Competition or to individuals who engage in fitness activities but do not compete at all.

Moreover, according to the Code, if a particular anti-doping rule violation is committed by any Athlete over whom an ADO has elected to exercise its authority to test and who competes below the international or national level, then the consequences set forth in the Code must be applied. In this regard, it should be highlighted that the Code and its International Standards lay down a complex set of rules which requires Athletes and Athlete Support Personnel to furnish a significant amount of Personal Information to ADOs and WADA, such as those related to Testing and Sample analysis, Whereabouts information, Athlete Biological Passport, Therapeutic Use Exemptions, Anti-doping rule violations, etc.

In accordance with the data protection legislation principles of proportionality, necessity and data minimisation, the related processing activities carried out by ADOs and WADA should not go beyond what is strictly necessary and proportionate for the purposes of preventing and fighting against doping in sport (cf. the 2005 UNESCO International Convention which has been ratified by the majority of the EU Member States in order to endorse the work of WADA at international level). In this context, it is essential that in deciding to extend their anti-doping program to sportsmen and sportswomen who compete below national level, National ADOs rely on a proper and rigorous assessment of the relevant risks of doping in a sport or in a sport discipline in accordance with the tools provided by the Code and

---

<sup>1</sup> International Standard for the Protection of Privacy and Personal Information (ISPP) and International Standard for Testing and Investigation (ISTI).

<sup>2</sup> 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)

<sup>3</sup> Second Opinion 4/2009 on the World Anti-Doping Agency (WADA) International Standard for the Protection of Privacy and Personal Information, on related provisions of the WADA Code and on other privacy issues in the context of fight against doping in sport by WADA and (national) anti-doping organizations.

its Standard with a view to identifying high risk athletes to be targeted for controls (cf. International Standard for Testing, notably 4.2 and 4.3).

In the light of the above, the Board considers that extending the scope of the Anti-doping Code and its International Standards to recreational-level Athletes (who engage in fitness activities but never compete) would be seen, as a general rule, as a disproportionate interference with the right to privacy and to protection of personal data of the concerned Athletes.

### [The Standard is not legally binding \(cf. Art. 29 WP's Letter to WADA of 5th March 2013\)](#)

The International Standard for the Protection of Privacy and Personal Information (hereinafter ISPPI) in its Article 4.1 mentions the principle according to which the common minimum set of rules established by the standard applies to all ADOs (including WADA) without prejudice to stricter rules or norms they may have to observe pursuant to their applicable data protection and/or privacy legislation. However, the comment related to the same Article clarifies that ADOs (including WADA) must comply with the said set of rules, provided that such compliance does not breach other applicable laws. In cases where such compliance may cause an ADO (or WADA) to breach other applicable laws, those laws shall prevail (see also, in the same direction, Article 5.1).

This means that the Standard which completes the World Anti-Doping Code with regard to data protection and/or privacy issues, is not legally binding. In particular, where applicable laws lay down provisions contrary to the safeguards on privacy and data protection provided by the Standard, these safeguards will not take precedence. This would not be a problem when the national applicable law sets a higher standard of protection for personal data than the one set forth in the Standard but it would be a cause of concern, if the ADO is obliged to apply a law setting a lower level of protection.

In these cases, it could be of particular relevance to require that the concerned ADO has to refer the matter to WADA and to the other ADOs without delay, so that these latter can take the appropriate measures in order to properly protect the data and/or the privacy of the affected Athlete or other concerned Person.

### [Communicating the DPO's contact information should be mandatory \(cf. Art. 29 WP's Letter to WADA of 5th March 2013\)](#)

The ISPPI in its article 4.5 provides for the designation of a "Person" by ADOs and WADA who is accountable for compliance with the Standard and local applicable laws, included data privacy laws. This person may be regarded as a Data Protection Officer (DPO) as described in the articles 37 to 39 of GDPR and should not be personally responsible in case of non-compliance with the GDPR<sup>4</sup>.

Notably, the Board regrets that the communication of the DPO's name and contact information is not mandatory and subject to a request from the Athlete or from the other concerned Person. Conversely, the communication of the DPO's contact details should have to be ensured to data subjects - as nevertheless required by Article 7.1 of the ISSPI - in order to make Athletes and other concerned Persons aware of existence of a DPO as well as of the chance to contact him/her with regard to all issues related to the processing of their personal data.

---

<sup>4</sup> Guidelines on Data Protection Officers ('DPOs'), p.4

## [The principle of data minimisation must not be derogated](#)

Regarding Article 5.3 of the ISSPI, we regret that the principle of data minimisation outlined in this provision may be derogated if “otherwise permitted or required by the Code”. This means that the safeguards on privacy and data protection set forth in the Standard will not be applicable if the rules of the Code lay down provisions which are contrary to them and -what is even more serious - that the Code itself does not seem to be fully in line with the Standard. As mentioned in Art. 29 WP’s earlier opinions, we are strongly in favour of the decision to promote the protection of privacy and personal data in the context of anti-doping activities which transpires in the Standard.

Nevertheless, we wonder whether the ISSPI will ensure effective compliance with the rules governing the protection of individuals' fundamental rights and freedoms, considering that the provisions outlined in the Standard will not even take precedence over the Code.

## [Clarify the grounds for processing \(cf. second Opinion 4/2009, 3.3 and Art. 29 WP’s Letter to WADA of 5th March 2013\)](#)

We observed that the ISPP in its Article 6 mentions different legal grounds to process personal data. Processing of personal data may be either based on a “valid legal ground”) or on the “Participant’s or other Person’s consent”. It is not however entirely clear under what circumstances a “valid legal ground” or a “consent” should be required. This point should be clarified.

Regarding consent, as mentioned in the Article 29 WP’s second Opinion 4/2009, 3.3, the requirement of such a consent to process personal data (Art 6.1 ISPP), included sensitive data (Art. 6.3 ISPP) does not comply with article 6, 7 and 9 of GDPR. Indeed, although the ISSPI requires that such a consent “shall be informed, freely given specific and unambiguous” the sanctions and the negative consequences attached to a possible refusal by participants to consent to the processing of their personal information as required for the purposes of the Code may prevent them to give a truly free consent (in this regard, see Article 6.2 of the ISSPI). Therefore, the validity of such consent is problematic.

Moreover, consent requirement to process criminal convictions, sanctions and offences (Art. 10 ISPP) is not a valid legal ground according to Article 10 GDPR. Indeed, the processing of such data may be carried out only under the control of official authority or if suitable safeguards are provided under national or EU law. Therefore, ADOs are not allowed to process such data, neither by publishing them on the Internet nor by processing them in other registrations unless national law or EU law allow it and if suitable safeguards are provided.

Regarding a “valid legal ground”, a more appropriate lawful basis would be compliance with a legal obligation to which the controller is subject, in accordance with article 6(1)(c) GDPR.

## [Ensure appropriate information to data subjects \(cf. Art. 29 WP’s Letter to WADA of 5th March 2013\)](#)

Regarding the information to be provided to data subjects, in line with the wording of the other rules set forth in the Standard, it is appropriate to mention WADA, along with the ADOs, as one of the entities which has the responsibility to meet to this obligation in its capacity as controller.

Moreover, in relation to the elements that should be communicated to the Person to whom the personal data relates, we suggest aligning the list outlined in Article 7.1 of the ISSPI to the provisions of Articles 13 and 14 of the GDPR whether personal data have been obtained from the data subject or not..

In the latter case, where ADOs (including WADA) receive Personal Information from Third Parties, and not directly from Athletes or other concerned Persons, Article 7.2 of the ISSPI provides that data subjects have to be informed "as soon as possible and without undue delay".

In this regard, to ensure a higher degree of protection for individuals, we suggest fixing a more precise deadline, such as the expression "but at the latest within one month" or, if the personal data are to be used for communication with the data subject, "at the latest at the time of the first communication to that Person to whom the Personal Information relates" or if a disclosure to another recipient is envisaged, "at the latest when the personal data are first disclosed".

Lastly, the derogation to the obligation of providing such notice outlined in Article 7.2 should be reworded in stricter terms in order to ensure that notice to data subjects may be delayed or suspended where providing such notice "is likely to render impossible or seriously impair" an anti-doping investigation or the integrity of the anti-doping process.

#### [Disclosures of personal data have to be linked to doping \(cf. Art. 29 WP's Letter to WADA of 5th March 2013\)](#)

As to the conditions under which the disclosure of data by ADO's/WADA to Third Parties is authorised, Article 8.3. c) of the ISSPI does not specify whether the "criminal offence" or the "breach of professional conduct rules" must be qualified as doping or at least be doping-related, or whether it is any "criminal offence" or "breach of professional conduct rules". As mentioned in Art. 29 WP's letter to WADA of 5th March 2013, we are of the opinion that it cannot be any criminal offence or breach of professional conduct rules, and that they have to be closely linked to doping. These limitations should be added to the text.

#### [Use a stricter deadline for notification of security breaches \(cf. Art. 29 WP's Letter to WADA of 5th March 2013\)](#)

With regard to the deadline for the notification of Security Breaches to the affected data subjects, Article 9.5 of the ISSPI requires that they must be informed by the responsible ADO/WADA "as soon as reasonably possible once the ADOs or WADA becomes aware of the details of the Security Breach". In this context we suggest however using a stricter deadline, such as the expression "without undue delay" that would contribute to ensure a higher degree of protection for individuals, particularly when this provision has to be applied in different legal and cultural contexts.

#### [Consider data protection impact assessment prior to the processing](#)

The ISPP in its article 9.6 plans that ADOs and WADA "shall regularly assess their processing of sensitive data information and whereabouts information to determine the proportionality and risks of their processing (...)."

We would also recommend taking into consideration the Article 35 GDPR and the EDPB guidelines concerning the realisation of a data protection impact assessment "*prior to the processing*"<sup>5</sup>, which could be suggested to ADOs/WADA, where not necessary under applicable laws, as a best practice. This tool allows controllers to take measures to address the risks to the rights and freedoms of the data subjects in relation to all processing operations which present high risks to those rights and freedoms and, therefore, not necessarily only when the processing concerns Sensitive Personal Information or Whereabouts Information.

#### Define maximum retention times (cf. second Opinion 04/2009, 3.5. and Letter to WADA of 5th March 2013)

Maximum retention times have been set up in the Annex A of the ISPPI: respectively 18 months and 10 years, depending on the nature of the data and the necessity and proportionality to keep those data. However, for some particular data, no maximum retention time has been defined which is not consistent with the principle of storage limitation. Indeed, it is planned to retain some data indefinitely (for instance, whereabouts only in case of disciplinary ruling or other ABP documents, disciplinary ruling data).

The possibility to retain such sensitive data for an indefinite time is not compliant with the legislation on data protection set forth in the GDPR. A maximum retention time should be defined according to the principles of necessity and proportionality. It should also be considered that, according to Article 4.4. of the ISPPI, ADOs/WADA shall maintain under their responsibility a record of the Processing which will also describe, amongst other elements, the period for which the Personal Information will be stored or the criteria used to determine this period. The same indications have also to be provided to data subjects according to Article 7.1 of the ISPPI. Concerning the retention time of samples which are considered as sensitive data under GDPR, the Annex A of the International Standard Protection on Privacy and Personal Information (ISPPI) indicates that « *samples [which] are anonymous, (...) may be retained indefinitely for scientific purposes* ».

In this regard, we would like to stress the impossibility to definitively de-identify urine or blood samples due to its biological nature. Indeed, biological samples (urine/blood samples) contain the person's DNA and the re-identification of the athlete cannot be excluded in any event. This is also the reason why a maximum retention period for samples shall be fixed to protect athlete's privacy.

According to Article 4.7.3 of the International Standard for Testing and Investigations, in order to define a retention strategy, ADOs should take into account « *the possible need for retroactive analysis in connection with the Athlete Biological Passport program* », « *new detection methods to be introduced in the near future relevant to the Athlete, sport and/or discipline* » or « *any other information made available to the Anti-Doping Organization* ». However, these criteria are not sufficient to justify an indefinite retention of samples. An adequate retention period for samples should be considered. For example: Is the retention of a sample for an indefinite period still relevant once an athlete retired or after expiration of the limitation period for proceedings?

---

<sup>5</sup> Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/6, p.17

## [The right of access to personal information is derogated \(cf. Art. 29 WP's second Opinion 4/2009, 3.2.6\)](#)

The ISSPI in its Article 11.1 provides that, in certain cases, data subjects are not entitled to exercise the right of access to personal information. As highlighted in Art. 29 WP's second Opinion 4/2009, the derogation is formulated in particularly vague terms and it does not, on the face of it, appear to be in conformity with the data protection legislation set forth in the GDPR. In this respect, we confirm that there would not a priori be a reason to withhold access to information on data in connection with «*the integrity of the anti-doping system or ADOs'/WADA's ability to plan or conduct No Advance Notice Testing or to investigate and establish anti-doping rule violations or other legal claim*».

In addition, Article 11.2 provides that in certain circumstances, the ADOs/WADA are not obliged to answer access request if it “*imposes a disproportionate burden on the Anti-Doping Organizations/WADA in terms of cost or effort given the nature of the Personal Information in question*”. As already mentioned, Art. 29 WP's second Opinion 4/2009, this exception does not appear to be in conformity with the data protection legislation.

In relation to both article 11.1 and 11.2, the Boards notes that any restriction of the right of access is only allowed if it conforms to the provisions of Article 23 of the GDPR which authorises Member States to adopt legislative measures aiming to restrict the scope of this obligation insofar as this restriction respects the essence of the fundamental rights and freedoms of individuals and is a necessary and proportionate measure in a democratic society. Therefore, the refusal of exercise of the right of access by the data subjects, set out in Article 11.3 of the ISSPI, is permissible only under the conditions of Article 23 of the GDPR, which must be interpreted strictly.

Lastly, the Board stresses once again that the Code should contain a right of remedy and a right of compensation for the damage suffered by the Athletes or other concerned Persons as a result of a processing operation incompatible with the Standard.

## [Publication on the Internet must be proportionally \(Art. 29 WP's second Opinion 4/2009 3.6 and Letter to WADA of 5th March 2013\)](#)

Regarding the unselective and automatic publication of all anti-doping rule violations on the Internet for the duration of one month or the duration of the athlete's ineligibility, provided by Articles 14.3.2 and 14.3.5 of the Code, we still refer to the Art.29 WP's second Opinion 4/2009 (par. 3.6) and the letter to WADA of 5ht March 2013 concerning the proportionality to use Internet as a proper diffusion channel for reporting publicly all anti-doping rule violations, without regard to the specific facts and circumstances of the case.

Similar concerns can be raised with regard to Article 14.4 of the Code that provides that ADOs may publish statistical reports of their Doping Control activities, showing the name of each Athlete tested and the date of each Testing.

As the Article 29 WP has outlined in its previous contributions, the Board suggests that public reporting should not be automatic and mandatory but, according to the principles of necessity, proportionality and data minimisation, should depend on the facts and circumstances of the case. As for the aspects that could be considered in order to determine whether the publication of an anti-doping rule violations is proportionate, we still refer to the elements mentioned by Article 29 WP in the letter to WADA of 5ht March 2013.

## Establish appropriate safeguards when re-using data for research

The WADA Code provides for the possibility to make further researches on samples after the written athlete's consent has been obtained (Article 6.3 WADA Code). This could be consistent with Article 9.2 of the GDPR (consent is required to process sensitive data – unless the consent cannot be specific, informed and unambiguous or it is not freely given, for example because the data subject has no genuine or free choice or is unable to refuse or withdraw consent at any time without detriment ). However, re-use of health data for research purposes may be subject to appropriate safeguards for the rights and freedom of data subjects, in accordance with Article 89 of the GDPR.

The Code mentions in its Art 19.2 that "*relevant anti-doping research may include, for example, sociological, behavioural, juridical and ethical studies in addition to medical, analytical and physiological investigation*". We express doubts about the necessity and the legitimacy for further researches on samples in the anti-doping fight as described in Article 19.2 of the Code. WADA should be more precise in defining what may include "relevant anti-doping research" on samples as well as in identifying the purposes of analysis of samples such as in Article 6.2 of the Code.

## Transfer of personal data to Law Enforcement Authorities (Letter to WADA of 5th March 2013)

With regard to transfers made from an EU ADO to the ADAMS database, as they take place in the context of the adequacy decision with Canada concerning the PIPEDA (and subsequent onward transfers to foreign law enforcement authorities or disclosures in the context of the laws governing access by law enforcement or national security authorities), the EDPB recalls that this adequacy decision shall remain in force until amended, replaced or repealed, if necessary, by a new Commission Decision as provided for under the GDPR (Article 45.9). Provided that the outcome of the ongoing assessment of the adequacy decision in question confirms that the level of protection ensured by the PIPEDA is adequate, also in relation to onward transfers and to access to these data by public authorities, notably for law enforcement and national security authorities, the EDPB is of the view that transfers taking place on this basis will continue to be valid.

As to the conditions under which the disclosure of data by ADO's/WADA to Third Parties is authorised, the EDPB notes that such disclosures within the same legal framework are subject to the applicable national laws and regulations, as it is further explained in the comment accompanying Article 8.3. c) of the ISSPI. In view of the importance of that condition, it would thus seem to be preferable to clarify this aspect in the Art. 8.3 c ISPP, rather than in the comment.

Also, Art. 8.3 c) ISPP does not specify whether the "criminal offence" or the "breach of professional conduct rules" must be qualified as doping or at least be doping-related, or whether it is any "criminal offence" or "breach of professional conduct rules". As mentioned in Art. 29 WP's letter to WADA of 5th March 2013, we are of the opinion that it cannot be any criminal offence or breach of professional conduct rules, and that they have to be closely linked to doping. These limitations should be added to the text.

Sophie in 't Veld  
Member of the European Parliament

Brussels, 9 October 2019

**By email only**

Ref: OUT2019-0036

**Subject: Your letter to the EDPB of 30 July 2019**

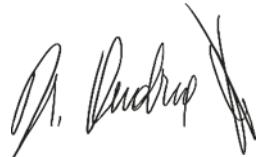
Dear Mrs. in 't Veld,

I would like to thank you for your letter dated 30 July 2019 with regard to the renegotiation of the EU PNR agreement with Canada and its impact on other PNR agreements. As you are probably aware, following up on the CJEU opinion of 26 July 2017 on the draft EU PNR agreement with Canada, the Working Party 29 (WP29) had sent in April 2018 a letter to the Commissioners Jourová, Avramopoulos and King, calling in particular on the European Commission to take action in order to ensure compliance with the CJEU's opinion of both PNR agreements with the U.S. and Australia, as many of the findings of the opinion were found to be equally relevant with regard to other PNR instruments. The WP29 had notably stressed that "*as the guardian of the EU treaty and thus of EU law, the European Commission is required to make all efforts necessary and to take all steps necessary to ensure compliance of all PNR instruments with the requirements set by the CJEU in its opinion as soon as possible*".

With regard to your question on the issue of onward transfers, I would also like to recall that the WP29 stated in its letter that "*with a view to the other PNR agreements, Art. 19 of the PNR agreement with Australia and Art. 17 of the PNR agreement with the U.S. include - in part – detailed provisions on onward transfers. Both of them, however, do not provide for the limitations expressed by the CJEU*". The WP29 added that "*the natural understanding of the CJEU opinion would be that onward transfers to other third countries also benefiting from a PNR agreement with the EU could only take place where both PNR agreements in place are in compliance with the Charter of Fundamental Rights as interpreted by the CJEU. In consequence, PNR data could only be further transferred from Canada to the U.S. or, vice versa, from the U.S. to Canada, once both of the PNR agreements are in line with the Charter of Fundamental Rights as interpreted by the CJEU*".

As regards the question whether the new draft for a PNR agreement with Canada provides for sufficient guarantees in order to address the deficits identified by the CJEU in its opinion, we are currently not in a position to comment due to the fact that a written draft has not been shared with us yet. We have only been orally briefed at working level on the progress achieved and the finalization of the negotiation. In this regard, the EDPB stands ready to issue an opinion on the new draft, once we have it, which would also allow to further answer the questions you raised in your letter.

Yours sincerely,

A handwritten signature in black ink, appearing to read "A. Jelinek".

Andrea Jelinek

Johannes Gungl

BEREC Chair 2018

Jeremy Godfrey

BEREC Chair 2019

Brussels, 3 December 2019

Ref: OUT2019-0055

**Subject: Data protection issues in the context of Regulation (EU) 2015/2120**

Dear Mr Gungl, Dear Mr Godfrey,

I refer to your letter of 13 November 2018 regarding consultation of the European Data Protection Board ('EDPB') on some issues on traffic management and zero-rating that concern privacy aspects, also in connection with Regulation (EU) 2016/679 ('GDPR') and Directive 2002/58/EC ('ePD').

In the attached Annex, you will find the Board's replies to the questions submitted by BEREC concerning certain terminological elements, as well as applicable rules related to personal data processing and privacy and specific obligations regarding transparency, consent and legal conditions for the processing of personal data.

In summary, the Board wishes to point out that the terms "specific content" and "monitoring" are not explicitly defined in the data protection legislation currently in force. Nevertheless, this or similar terminology is in use in jurisprudence and important principles regarding general monitoring of communications have been set out in the case law of the Court of Justice of the European Union ('CJEU'). In particular, in Case C-70/10 *Scarlet Extended*, the Court and the Advocate General have undertaken a thorough analysis of traffic analysis and monitoring operations. The analysis of a filtering system in that case led to the conclusion that any such filtering system would create an interference with the fundamental rights established by Articles 7 and 8 of the Charter.

Furthermore, in order to determine whether and to what extent traffic monitoring may be lawful, Articles 4, 5 and 6 ePD are relevant. The ePD generally provides that communications related data may not be stored, tapped or otherwise intercepted without the consent of all end-users concerned<sup>1</sup>. In the case of a network service that is based on the internet protocol (IP), the EDPB is of the view that the IP header information constitute traffic data within the meaning of Article 2(b) ePD, and that all other parts of the packet must be considered content or

---

<sup>1</sup> The ePD provides for exemptions to this requirement in Art 5 ePD for "technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.", for "any legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication", in Art 6(2) ePD and in Art 15(1) ePD.

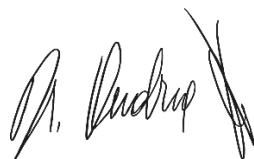
“specific content”. In some cases, transport headers could also be considered traffic data. The communications service provider must not process the content of an IP packet for purposes other than technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality, including elements serving as control information for other protocol layers, e.g. http headers or URLs. This interpretation appears to be reflected correctly in the BEREC’s Net Neutrality Rules (BoR (16) 127 69), as reported in BEREC’s letter.

As established in C-70/10 and C-582/14 *Breyer*, also traffic data (including IP addresses) constitute personal data when associated to a natural person. Consequently, the relevant GDPR provisions apply<sup>2</sup>. The GDPR transparency requirements complement those laid down in the Regulation (EU) 2015/2120 (hereinafter “*TSM Regulation*”)<sup>3</sup> Article 4, which have a different scope and purpose. Furthermore, the GDPR’s definition of ‘consent’ and its provisions on consent also apply in cases where the ePD requires consent.

As BEREC correctly recognizes in its letter, the ePD requires consent for the processing of traffic data of all end-users concerned in order to provide value added services. It should be taken into account that the domain names and URLs can provide revealing insights on a wide variety of aspects of a person’s life. For reasons set out in the annex, the Board considers that **processing of data such as the domain name and URL by internet access services providers for traffic management and billing purposes is unlawful, unless consent of all users is obtained**. The EDPB remains open to discuss how traffic management and zero-rating offers could be also implemented using other technical means, such as those suggested in the annex.

Finally, the Board would like to thank the BEREC for this consultation on these very important data protection related issues.

Yours sincerely,



Andrea Jelinek

---

<sup>2</sup> EDPB 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

<sup>3</sup> Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and retail charges for regulated intra-EU communications and amending Directive 2002/22/EC and Regulation (EU) No 531/2012, OJ L 310, 26.11.2015, p. 1–18

## Annex

### a. Is the term “specific content” commonly used in privacy context, and how would this term in that case be defined in EU privacy rules?

#### Background

According to Regulation (EU) 2015/2120 (hereinafter “TSM Regulation”)<sup>4</sup> Article 3(3) ‘[the traffic management] measures shall not monitor the specific content and shall not be maintained for longer than necessary.’

The BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules defines ‘*specific content*’ as the transport layer protocol payload<sup>5</sup>. Therefore, both network layer (e.g. IP packet) headers and transport layer (e.g. TCP or UDP) headers are considered generic content.

#### Answer

Both traffic data and content are part of the communications data as defined by article 2 ePD.

There is no definition of the term ‘*specific content*’ neither in the ePrivacy Directive<sup>6</sup> (‘ePD’) nor in the GDPR<sup>7</sup>.

Article 2 ePD defines the term ‘*communication*’ as ‘any information exchanged or conveyed between a finite number of parties by means of publicly available electronic communication service (...).’ ‘*Traffic data*’, are defined as “any data processed for the purpose of conveyance of a communication on an electronic communication network or for the billing thereof.”

The EDPB considers that network layer (e.g. IP packet) headers and transport layer (e.g. TCP or UDP) headers should be considered traffic data, while the transport layer protocol payload should be considered contents of the communication.

---

<sup>4</sup> Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and retail charges for regulated intra-EU communications and amending Directive 2002/22/EC and Regulation (EU) No 531/2012, OJ L 310, 26.11.2015, p. 1–18

<sup>5</sup> 69. In assessing traffic management measures, NRAs should ensure that such measures do not monitor the specific content (i.e. transport layer protocol payload).

70. Conversely, traffic management measures that monitor aspects other than the specific content, i.e. the generic content, should be deemed to be allowed. Monitoring techniques used by ISPs which rely on the information contained in the IP packet header, and transport layer protocol header (e.g. TCP) may be deemed to be generic content, as opposed to the specific content provided by end-users themselves (such as text, pictures and video).

<sup>6</sup> Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201, 31.7.2002, p. 37–47

<sup>7</sup> 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. 1–88

**b. Is the term “monitoring” commonly used in privacy context, and how would this term in that case be defined in EU privacy rules?**

**Background**

The term ‘monitor’ or ‘monitoring’ is used in Recital 10<sup>8</sup> and Article 3(3) of the Regulation (EU) 2015/2120. In both cases the monitor term is used in the context of IAS providers’ traffic management activities while preventing the monitoring of ‘specific content’.

The BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules also refers to monitoring in its paragraph 85, where it is described as ‘monitoring of the integrity and security of the network’.

**Answer**

Although the term ‘monitoring’ is commonly used in the context of privacy and data protection, there is no definition of the term neither in the ePD nor in the GDPR which would apply in the present context.<sup>9</sup>

However, general principles for monitoring of communications have been developed in the case law of the Court of Justice of the European Union (‘CJEU’). For example, the case C-70/10 *Scarlet Extended*<sup>10</sup>, which involved balancing the protection of fundamental rights: on the one hand, the protection of the intellectual property right enjoyed by copyright holders, and, on the other hand, that of the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart information . In this case the CJEU ruled that “*Preventive monitoring (...) would (...) require active observation of all electronic communications conducted on the network of the ISP concerned and, consequently, would encompass all information to be transmitted and all customers using that network*”. In this case, the Court and the Advocate General undertook a thorough analysis of traffic analysis and monitoring operations. The analysis of a filtering system in that case led to the conclusion that any such filtering system would create an interference with the fundamental rights established by Articles 7 and 8 of the Charter. As the AG recognized in his opinion<sup>11</sup>, this interpretation was also held by the European Data Protection Supervisor<sup>12</sup> (EDPS) and the

---

<sup>8</sup> Recital 10 of Regulation (EU) 2015/2120. ‘Reasonable traffic management does not require techniques which monitor the specific content of data traffic transmitted via the internet access service.’

<sup>9</sup> In the context of the GDPR, “monitoring” individuals’ habits or preferences is one of the situations that trigger high risks for data subjects’ rights and freedoms to the extent that a prior data protection impact assessment is mandatory before a processing operation entailing a “monitoring” is put in place, see e.g. Art. 3(2) b) or Art. 35 (3) c GDPR.

<sup>10</sup> Judgement of the Court of Justice of the European Union of 24 November 2011, Case C-70/10, Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), ECLI:EU:C:2011:77

<sup>11</sup> Opinion of Advocate General Cruz Villalón delivered on 14 April 2011, Case C-70/10, Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)), ECLI:EU:C:2011:255

<sup>12</sup> Opinion of the European Data Protection Supervisor of 10 May 2010 on the proposal for a directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA (OJ 2010 C 323, p. 6, paragraph 11).

Article 29 Working Party (WP29), the predecessor of the European Data Protection Board (EDPB)<sup>131415</sup>.

**c. Which rules follow from EU privacy law for practices concerning traffic management?**

Background

According to Article 3(4) of the Regulation (EU) 2015/2120 processing of personal data shall be carried out in accordance with the ePD and with the Directive 95/46/EC (since replaced by Regulation (EU) 2016/679 (GDPR)).

Answer

Recital 9 of the TSM Regulation provides that '*[t]he objective of reasonable traffic management is to contribute to an efficient use of network resources and to an optimisation of overall transmission quality responding to the objectively different technical quality of service requirements of specific categories of traffic, and thus of the content, applications and services transmitted.*'

The EDPB understands that by "*traffic management*" one should intend an intervention of the network operator so that, based on predefined criteria communications flowing into the network are routed in a different way. Recital 9 of the TSM Regulation clarifies that such routing '*differentiation should be permitted only on the basis of objectively different technical quality of service requirements (for example, in terms of latency, jitter, packet loss, and bandwidth) of the specific categories of traffic, and not on the basis of commercial considerations*'. From a privacy and data protection perspective, processing that involves scrutiny of packet flows might amount to monitoring of electronic communications and must be approached with caution. In addition, the choice of criteria for traffic management is important, since this is where the impacts on individuals' rights and freedoms may be generated.

In the context of traffic management, it is particularly important to highlight that the content of communications and the traffic data are both protected by the right to the confidentiality of communications, which is a fundamental right, guaranteed by Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and Article 7 of the Charter of Fundamental Rights of the European Union.

---

13 Case C-70/10 Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) [2011] ECLI:EU:C:2011:255, Opinion of AG Cruz Villalón, para 76

14 EDPS Opinion of the European Data Protection Supervisor of 22 February 2010 on the Anti Counterfeiting Trade Agreement (ACTA), OJ 2010 C 147, p. 1, paragraph 24; EDPS Opinion of the European Data Protection Supervisor of 10 May 2010 on the proposal for a directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, OJ 2010 C 323, p. 6, paragraph 11

15 Article 29 Working Party "Privacy on the Internet - An integrated EU Approach to On-line Data Protection-" WP 37, 21 November 2000, p. 22

Confidentiality is further protected in secondary EU legislation, in particular, Article 5 ePD. Article 5 (1) ePD sets out the general rule that ‘*(...) listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users*’ is prohibited without the consent of the users concerned, allowing two exceptions, a legal authorisation in line with ePD Article 15(1) and the ‘*technical storage which is necessary for the conveyance of a communication*’.

Article 6 (2) ePD allows the processing of traffic data for the purposes of subscriber billing and interconnection payments.

Article 2(b) defines “traffic data” as “any data processed for the purpose of conveyance of a communication on an electronic communications network or for the billing thereof”.

Further, Article 5(1) states in respect of national legislative measures on confidentiality of communications that they “...shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.”

In order to benefit of this last exception for traffic management, the processing should be clearly demonstrable as being strictly necessary and proportionate. To be strictly necessary, such data processing should be required, unconditional and without alternative. To be proportionate, the processing should strike the right balance between the means used and the intended aim. Service providers need to be able to provide this demonstration whenever and however they under-take such processing.

On this aspect, it is worth recalling that the processing of personal data retained in the context of traffic management must also respect other principles that derive from the GDPR and the ePD. In particular, the data minimization principle (personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed), and the principle of lawfulness, fairness and transparency (personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject).

In addition, as the ePD complements and particularises the GDPR and Art 2(f) ePD refers to the definition of consent in GDPR<sup>16</sup>, whenever the two exceptions in articles 5(1) and article 6(2) do not apply and consent is the legal basis for the processing, this must be interpreted in line with Article 4 (11) GDPR as ‘*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*.’ The Article 29 Working Party’s guidelines on consent<sup>17</sup> provide general guidance on how to obtain users consent.

<sup>16</sup> 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]”

<sup>17</sup> Article 29 Working Party. “Guidelines on Consent under Regulation 2016/679” adopted on 28 November 2017, last revised and adopted on 10 April 2018, 17/ENWP259 rev.01 - endorsed by the EDPB

**d. How would the obligation to be transparent on traffic management measures relate to obligation to inform under EU privacy law?**

**Background**

According to Article 4(a) of the Regulation (EU) 2015/2120, '*providers of IAS shall ensure that any contract specifies [...] the information on how traffic management measures applied by that provider could impact on the quality of the internet access services, on the privacy of end-users and on the protection of their personal data.*'

**Answer**

Providers of IAS must also provide their customers with the information foreseen in Articles 12 and 13 GDPR. The purposes for which Regulation (EU) 2015/2120 allows traffic monitoring (compliance with *legislative acts, preservation of network integrity and security and prevention or mitigation of network congestion*) are different from the purpose of fulfilling the contract or conveying the message. The subscriber should be informed of such purposes and of the associated legal grounds envisaged in ePD. Such information should be provided in a precise, transparent, comprehensible and easily accessible form. It may be provided together with the contractual terms.

Furthermore, providers of IAS bear a responsibility for informing customers about any update or changes to their traffic management policies.

**e. When applying traffic management for IAS, from a data protection perspective, is it allowed to process data such as the domain name and URL?**

**Background**

Article 3(4) of the Regulation (EU) 2015/2120 sets out the requirements to process personal data for traffic management.

On the one hand it requires that the processing will be carried out in accordance with the ePD and with the GDPR. On the other it allows such processing only if necessary and proportionate to achieve the objectives set out in Article 3(3) paragraph 3 of the Regulation (EU) 2015/2120.

**Answer**

The confidentiality of communications enshrined in Article 5(1) ePD, as said, prohibits '*technical storage which is necessary for the conveyance of a communication*' without the consent of the users concerned, allowing two exceptions: a legal authorisation in line with ePD Article 15(1) or for the '*technical storage which is necessary for the conveyance of a communication*'.

The relevance of confidentiality is of high importance as the domain names and URLs, in conjunction with other data relating to electronic communications, can provide revealing insights on a wide variety of aspects of a person's life. In fact, they can be as revealing as the actual contents of the communication.

IAS service providers do not require information included in the transport layer payload (like domain names or URLs) to convey a communication on an electronic communication network.

Therefore, domain names and URLs cannot be considered ‘traffic data’ as defined in Article 2(b) ePD and they cannot be processed under the provisions in Article 6 ePD.

Article 5(1) ePD allows for the ‘*technical storage which is necessary for the conveyance of a communication*’. However, domain names and URLs are not necessary for IAS service providers to convey a communication.

Even the option of basing traffic management on consent is not unconstrained. Consent, in fact, must be interpreted in the light of Article 4 (11) GDPR as “*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.*”. In the light of this definition, no possibility exists for setting vague purposes, and any open-ended traffic management processing operations would be in breach of the law. IAS providers should also consider that freely given consent can be withdrawn anytime. The Article 29 Working Party’s guidelines on consent<sup>18</sup> provide general guidance on how to obtain users consent.

The EDPB considers that the processing of communications and related traffic data on the basis of the Article 5(1) ePD for purposes of traffic management requires the consent of all end-users of an IAS provider.

IAS providers would need to perform deep packet inspection to gain access to the domain names and URLs that are included in the transport layer payload.

As already mentioned, a filtering system that would require an ISP to carry out general monitoring of the information in Case C-70/10 Scarlet Extended led the CJEU to the conclusion that any such filtering system would create an unjustifiable interference with the fundamental rights established by Articles 7 and 8 of the Charter.

Considering the interference that the general monitoring of end-users’ communications content would create, **the EDPB is of the view that the use of deep packet inspection to extract the domain names and URLs for traffic management is unlawful, unless consent of all users is obtained.**

IAS provider could achieve the objectives of traffic management standardizing and using data available at the IP header like the Explicit Congestion Notification<sup>19</sup> (ECN) or the Differentiated Services Code Point<sup>20</sup> (DSCP). Therefore, the EDPB is of the view that processing of domain names and URLs by providers of IAS is not necessary to conduct traffic management.

The EDPB encourages the IAS providers and BEREC where relevant to define and agree on less invasive and more standardized ways to manage internet traffic, interoperable throughout different IASs, which are not based on the use of URLs and domain names.

---

<sup>18</sup> Article 29 Working Party “Guidelines on Consent under Regulation 2016/679” adopted on 28 November 2017, last revised and adopted on 10 April 2018, 17/ENWP259 rev.01 - endorsed by the EDPB

<sup>19</sup> <https://tools.ietf.org/html/rfc3168>

<sup>20</sup> <https://tools.ietf.org/html/rfc2474>

**f. On zero-rating offers, how can providers of IAS obtain user consent on monitoring all visited domain names and websites for billing purposes?**

Background

According to the BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules<sup>21</sup>, a zero-rating offer ‘is where an ISP applies a price of zero to the data traffic associated with a particular application or category of applications (and the data does not count towards any data cap in place on the IAS).’

Answer

Art 5(1) ePD prohibits ‘listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.’

If billing is the purpose of the processing of electronic communication data, legislative measures referred in Article 15(1) ePD would not be applicable. Consequently, freely given and specific consent of the users would be required to process visited domain names and websites for billing purposes<sup>22</sup>.

As mentioned in the previous answer, domain names and URLs cannot be processed under the traffic data provisions in Article 6 ePD.

For the mentioned purpose, the IAS will need to obtain consent of all end-users. The same argument as provided in the answers to question c and e relating to consent still apply in this case<sup>23</sup>.

For an IAS to obtain consent in a way that will fully meet all the requirements stipulated by the GDPR will be challenging.

For the same reasons expressed in the previous answer, the EDPB is of the view that **monitoring all visited domain names and websites for billing purposes is unlikely to be possible in a lawful manner.**

---

<sup>21</sup>[https://berec.europa.eu/eng/document\\_register/subject\\_matter/berec/download/0/6160-berec-guidelines-on-the-implementation-b\\_0.pdf](https://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/6160-berec-guidelines-on-the-implementation-b_0.pdf)

<sup>22</sup> Article 29 Working Party “Guidelines on Consent under Regulation 2016/679” adopted on 28 November 2017, last revised and adopted on 10 April 2018, 17/ENWP259 rev.01 - endorsed by the EDPB

<sup>23</sup> The Art 29 Working Party Guidelines state “that the controller must ensure that consent can be withdrawn by the data subject as easy as giving consent and at any given time.” (emphasis added)

- g. On zero-rating offers, how can providers of IAS lawfully monitor traffic of third parties for billing purposes (red arrow in the figure above)?

Answer

As mentioned in the reply to the previous question, Article 5(1) ePD requires the user's consent to legitimise the processing.

The EDPB is of the view that whenever non-contractual parties are involved, consent as in art 5(1) ePD is needed to legitimise the processing.

Consent must be obtained from all users involved in the processing of communications data (senders and recipients)<sup>24</sup>. Therefore, according to Article 5(1) ePD, the legal ground to monitor traffic for billing purposes can only be consent of all involved end-users (to be understood as the individuals actually using the service).

In the case of the communication represented by the red arrow in the figure, the sender of an electronic communication has not consented the monitoring of his or her traffic. Therefore, **monitor of traffic of such third parties for billing purposes would be unlawful**.

The data contained in headers of transport, network or data link layers, if properly standardized, could be considered traffic data and processed by the IAS providers for billing purposes in line with the provisions in Article 6 ePD. However, following the data minimization principle, the data included for billing purposes in the mentioned headers should be adequate, relevant and limited to what is necessary (e.g. to count or not a packet against the data cap).

Again, the EDPB encourages the IAS providers and BEREC where relevant to define and agree on less invasive and more standardized ways to bill internet traffic, based on labelling the type of communication, interoperable throughout different IASs, which are respectful of the data minimization principle and do not require traffic monitoring.

---

<sup>24</sup> See also 29 Working Party Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), WP 247, p.3 and p.13

Patrick Breyer  
Member of the European Parliament

Brussels, 31 March 2020

By email only

Ref: OUT2020-0024

Dear Mr. Breyer

I would like to thank you for your email dated 22 January 2020 on the data retention case within the Danish national police. The Danish Data Protection Agency has informed the EDPB that it has opened a case investigating the matter. EDPB members will take due account of the conclusion of the Danish Data Protection Agency investigation.

As regards the question on the necessity for further investigations of other Member States' IT systems used in processing communications data, the EDPB notes that the false communication data in this case related to deficiencies in an internally developed IT system of the Danish National Police. However, the content of the case highlights the importance and the need for software to adhere to the principles of data protection and the obligation of Data Protection by Design and by Default. I would like to recall the EDPB adopted guidelines 4/2019 on Article 25 Data Protection by Design and by Default on 13 November 2019. The guideline specifies the requirement for controllers to *"implement appropriate technical and organisational measures and necessary safeguards, designed to implement data protection principles in an effective manner and to protect the rights and freedoms of data subjects."* The interpretations provided in this guideline on Article 25 of the GDPR equally apply to Article 20 of Directive (EU) 2016/680.

Yours sincerely,



Andrea Jelinek

Mark W. Libby  
Chargé d’Affaires, a.i.  
United States Mission to the European Union,  
Zinnerstraat 13,  
B-1000 Brussels,  
Belgium

24 April 2020

Ref: OUT2020-0029

Dear Mr. Libby,

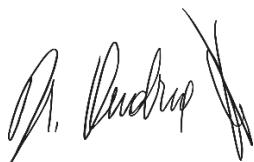
Thank you for your letter dated 9 April 2020 raising a question on the transfer of personal data for the purpose of scientific research and the development of vaccines and treatments to combat COVID-19 on the basis of the “important public interest” derogation in Article 49 (1) (d) of the GDPR.

I am pleased to inform you that the European Data Protection Board adopted guidelines on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak on 21 April 2020, which address the question raised in your letter.

Therefore, I kindly invite you to read our Guidelines 03/2020, in particular Section 7 on international data transfers, available via the following link: [https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032020-processing-data-concerning-health-purpose\\_en](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032020-processing-data-concerning-health-purpose_en).

As expressed in these guidelines, the GDPR does allow for meaningful collaboration between EEA and non-EEA public health authorities and research institutions in the search for vaccines and treatments against COVID-19, while simultaneously protecting the fundamental right to data protection in the EEA.

Yours sincerely,



Andrea Jelinek

Ďuriš Nicholsonová  
Member of the European Parliament

by e-mail only

Ref: OUT2020-0030

Dear Ms Ďuriš Nicholsonová, Dear Mr Jurzyca,

I would like to thank you for your letter dated 23 March 2020 with regard to the need for common guidance on the application of the General Data Protection Regulation (GDPR), and other relevant legal instruments of the EU in matters of data protection, in the fight against the COVID-19 pandemic.

As a preliminary remark, let me emphasise that the EDPB is extremely concerned about this emergency, and is fully committed to do whatever falls within the remit of its mandate and powers to help Member States reduce the virus spread.

The EDPB is aware that the COVID-19 outbreak is raising numerous questions concerning data protection and privacy issues, especially in the context of national Governments and private actors turning towards the use of data driven solutions to help fight the spread of the disease.

**In this context, I would like to highlight that data protection laws already take into account data processing operations necessary to contribute to the fight against an epidemic. Therefore, there is no need to lift GDPR provisions but just to observe them.** The EDPB has already issued guidance on data protection and privacy issues in this current crisis<sup>1</sup>, as have many of its Members. What public health authorities in the Member States are allowed to do depends on the tasks assigned to them by law. Similarly, what employers can do concerning their own staff depends largely on national labour laws. Notwithstanding any potential difference in these sector specific laws, **as regards data protection matters, the EDPB has already published guidelines on the issues of geolocation and other tracing tools<sup>2</sup>, as well as the processing of health data for research purposes<sup>3</sup> in the context of the COVID-19 outbreak.**

There are initiatives for apps and tools for voluntary self-tracking. A large variety of solutions are being developed. The EDPB has followed closely these developments and has already provided guidance on geolocation and other tracing tools for this purpose, as already mentioned. The national supervisory authorities are also closely following the issue at national level.

It is of the utmost importance **to preserve data protection principles even, and more importantly, in this difficult situation**. The data protection principles (including lawfulness, transparency, fairness, purpose limitation, data minimisation, accuracy, storage limitation and security) not only guarantee

---

<sup>1</sup> [Statement of the EDPB chair of 16 March 2020](#), [Statement of the EDPB of 19 March 2020](#), Letter to the European Commission of 15 April 2020

<sup>2</sup> [Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak.](#)

<sup>3</sup> [Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak.](#)

the protection of fundamental rights of our citizens, in line with our common European values and democracies, but also create trust in the governments who are looking into post-confinement data driven measures.

Finally, on the topic on additional legislative measures, should they be considered by Member States or at EU level, the **EDPB and its Members stand of course ready to provide advice to the legislators**, in line with articles 70 and 57 GDPR. Several Supervisory authorities are already in contact with the stakeholders looking into data-driven approaches.

**To conclude, maintaining transparency, data quality and trust is key for complying with the EU legal framework on data protection. They are also a key element of public acceptance of any measures enacted by governments and the take-up of initiatives proposed by private entities on a voluntary basis. Data protection rules ensure, among others, transparency, data quality and trust in a time where it is much needed in order for citizens to support the use of technology to fight the spread of the disease.**

Yours sincerely,



Andrea Jelinek

Sophie in 't Veld  
Member of the European Parliament

Ref: OUT2020-0031

by e-mail only

Dear Ms in 't Veld,

Thank you very much for your letter dated 3 April 2020 and its follow up letter dated 8 April 2020 in which you raise a series of questions regarding the latest technologies that are being developed in order to fight the spread of COVID-19.

The EDPB is following closely the rapid developments in relation to the initiatives and the measures taken by governments, public and private entities for the containment and mitigation of the current pandemic. In this context, the EDPB has already published a statement<sup>1</sup>, which outlined a number of considerations that should be taken into account so that lawful processing of personal data is ensured and data protection principles are respected.

The EDPB has further decided to prioritise providing guidance on the issues of geolocation and other tracing tools, as well as the processing of health data for research purposes<sup>2</sup> in the context of the COVID-19 outbreak.

Please be informed that the EDPB adopted during its 23rd Plenary Session on 21 April its guidance on the use of location data and contact tracing tools. The EDPB has taken into account concerns and queries from the stakeholders involved as well as the general public in the drafting of this document. We hereby annex the guidance to this letter.

We thank you for interest in the work of EDPB and wish to assure you that we will continue monitoring these developments closely and act proactively in the deliberation of our duties.

Yours sincerely,



Andrea Jelinek

Annex: Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak.

<sup>1</sup> [Statement by the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak](#).

<sup>2</sup> [Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak](#).

**Andrea Jelinek**  
Chair of the European Data Protection Board

rue Wiertz, 60  
1047 Brussels

Brussels, 03 June 2020

Ref: OUT2020-0046

**Subject: Letter of 11 May 2020 from the Civil Liberties Union for Europe, Access Now and the Hungarian Civil Liberties Union (HCLU)**

Dear Ms. Massé, Mr. Szabó and Mr. Dénes,

Thank you for your letter related to the adoption by the Hungarian government of the Decree 179/2020 of 4 May 2020 on the derogations from certain data protection and access to information provisions during the state of danger<sup>1</sup>.

The EDPB dedicates special attention to the measures involving the processing of personal data adopted in the context of the fight against COVID-19 pandemic. Let me recall in particular the recent adoption of the guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, the guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, the Statement on the processing of personal data in the context of the COVID-19 outbreak and the letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic.

In this context, and as already highlighted, the GDPR remains applicable and allows for an efficient response to the pandemic, while at the same time protecting fundamental rights and freedoms. Data protection law, including relevant applicable national law, already enables data-processing operations necessary to contribute to the fight against the spread of a pandemic, such as the COVID-19 pandemic.

The EDPB would like to recall that the rights of data subjects are an essential and integral part of the implementation of the fundamental right to data protection as enshrined in the Charter of fundamental rights of the European Union and are key to the implementation of the GDPR in the Union. In that sense, as laid down in Article 23 of the GDPR, any restriction to the rights of data subjects must respect the essence of the fundamental rights and freedoms and must be a necessary and proportionate measure in a democratic society to safeguard an important objective of general public interest of the Union or of a Member State. Even in these exceptional times, the protection of personal data must be upheld in all emergency measures, including restrictions adopted at national level, as per Article 23 of the GDPR thus contributing to the respect of the overarching values of democracy, rule of law and fundamental rights on which the Union is founded.

---

<sup>1</sup> Decree 179/2020 (V. 4.) Korm. rendelet a veszélyhelyzet idején az egyes adatvédelmi és adatigénylési rendelkezésektől való eltérésről (<https://net.jogtar.hu/jogszabaly?docid=a2000179.kor>).

With respect to supervision over restrictions on data subject rights and over compliance of Member States' data protection law with EU law, I would like to stress that the EDPB does not have the same competences, tasks and powers as national supervisory authorities and as the European Commission.

At national level, the assessment of alleged infringements of the GDPR falls within the competence of the responsible and independent national supervisory authority, subject to the cooperation and consistency mechanisms set out in the GDPR when applicable. Data protection supervisory authorities are responsible for monitoring and, if necessary, enforcing the application of data protection principles in the context of the state of emergency, including on the lawfulness of any restriction on the exercise of data subject rights. A judicial remedy should also always be available in accordance with Articles 78 and 79 of the GDPR.

At European level, under Article 70 of the GDPR, the EDPB has the power to advise the European Commission on any issue related to the protection of personal data in the Union and to examine any question covering the application of the GDPR in order to encourage its consistent application. According to Article 258 of the Treaty on the functioning of the European Union, only the European Commission may take legal steps against a Member State in case of a breach of EU law.

The EDPB is committed to ensure a full and consistent implementation of the GDPR throughout the EU and, to that end, will issue guidelines on the implementation of Article 23 of the GDPR in the coming months. In the meantime, the EDPB adopted a statement recalling main principles related to the restrictions on data subject rights in connection to the state of emergency in Member States. The statement is annexed to this letter. I wish to reassure you that the EDPB will continue to pay special attention to the developments of personal data processing and restrictions on data subject rights in connection to the state of emergency in Member States and will remain ready to support all members of the EDPB, including the Hungarian Supervisory Authority, in such matters.

Yours sincerely,



Andrea Jelinek

Maximilian Schrems  
Honorary Chair of noyb.eu  
NOYB – European Center for Digital Rights  
Goldschlagstraße 172/4/3/2  
1140 Vienna  
Austria

Brussels, 9 June 2020

Ref: OUT2020-0050

Dear Mr Schrems,

I refer to your letter we have received on 25 May 2020.

Since May 2018, during the last two years, the Board has been constantly working on the improvement of the cooperation between the Supervisory Authorities and the consistency procedures. As you know, tools and procedures to ensure the functioning of the one-stop shop mechanism have been put in place; and the Board has adopted several guidance to clarify the terms of the GDPR, as well as consistency opinions to ensure a consistent application of the law throughout the European Economic Area. We advised the EU legislators on a number of topics and the Supervisory Authorities already actively cooperate through the cooperation and consistency mechanism to deal with cross-border cases.

As part of its contribution to the evaluation of the GDPR under Article 97 published in February 2020, the Board has, at the same time, identified a number of issues requiring improvement. Differences in national administrative procedural laws, together with time and resources needed to resolve cross-border cases, have been considered by the Board as the main challenges to be addressed.<sup>1</sup>

The Board is committed to find solutions and address the challenges ahead where it lies within our competence<sup>2</sup>.

---

<sup>1</sup> For more information see the contribution of the EDPB to the evaluation of the GDPR under Article 97, available at: [https://edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-evaluation-gdpr-under-article-97\\_en](https://edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-evaluation-gdpr-under-article-97_en)

<sup>2</sup> Ibid, page 11: as part of its contribution to the evaluation of the GDPR, the Board has notably considered that “the one-stop-shop and the cooperation mechanism are still relatively new procedures. In order to better understand the potential obstacles and identify available solutions, the EDPB is undertaking in particular the following steps: further clarification of the applicable procedural steps in the case of Article 60GDPR; analysis of the different national administrative procedural laws and practices; further work towards a common interpretation of key concepts and terms of the GDPR one-stop-shop and the cooperation procedure; strengthening of the communication among the SAs; exploiting all the tools provided by the GDPR to enhance cooperation, including joint operations”.

The Board and all its members are fully committed in making use of all cooperation tools established by the GDPR and consider that the success of the EU regulatory model notably relies on an efficient and optimal functioning of the one-stop-shop mechanism.

Yours sincerely,



Andrea Jelinek



Juhan Lepassaar  
ENISA Executive Director  
1 Vasilissis Sofias Str.  
Marousi 15124, Attiki  
Greece

9 June 2020

Ref: OUT2020-0051

Dear Mr Lepassaar,

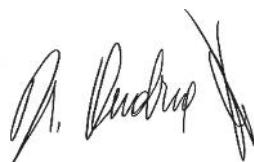
I thank you very much for contacting me on the matter of the ENISA Advisory Group. For the two-and-a-half year mandate for membership of the advisory group of ENISA, established in accordance with Article 21 of Regulation 2019/881 I hereby inform you that the EDPB representative is

J Dr. Gwendal LE GRAND  
Deputy secretary general  
Commission nationale de l'informatique et des libertés (CNIL)  
3 Place de Fontenoy, TSA 80715, 75334 PARIS CEDEX 07  
France  


Please be informed that I ask the EDPB Secretariat to notify to you the alternate representative in due time.

The EDPB is as well looking forward to collaborate with ENISA at future occasions on topics of common interest.

Yours sincerely,



Andrea Jelinek

Moritz Körner  
Member of the European Parliament

Brussels, 9 June 2020

**By email only**

Ref: OUT2020-0053

Dear Mr. Körner,

Thank you very much for your letter dated 6<sup>th</sup> of December 2019 in which you raise questions on the TikTok application, as a follow up to media reports regarding TikTok processing of personal data.

The EDPB is aware of the concerns that you have mentioned in your letter, and has already issued guidelines and recommendations that are to be taken into account by all data controllers whose processing are subject to the GDPR, in particular when it comes to transfer of personal data to third countries, substantive and procedural conditions for access to personal data by public authorities or the application of the GDPR territorial scope<sup>1</sup>. On this last point, the EDPB recalls that the GDPR applies to the processing of personal data by a controller, even if it is not established in the Union, where the processing activities are related to the offering of goods or services to data subjects in the Union.

While the EDPB cannot comment on possible ongoing investigations by its members, I would like to inform you that the EDPB has decided to establish a taskforce in order to better coordinate potential actions and to acquire a more comprehensive overview of TikTok's processing and practices across the EU.

We thank you for your continued interest on the work of the EDPB and assure you this matter will be considered with the greatest attention, in particular when it comes to processing of minors' personal data.

Yours sincerely,



Andrea Jelinek

---

<sup>1</sup> Available here : [https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version\\_fr](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_fr)

Ralf Bose  
Chair of the Committee of European Auditor Oversight Bodies  
By email only

16 June 2020

Ref: OUT2020-0060

Dear Mr Bose,

I am writing to you further to your e-mail addressed to the EDPB on 4 May 2020 regarding the topic of administrative arrangements for transfers of data being negotiated between the EU national auditor oversight bodies, members of the Committee of European Auditor Oversight Bodies (CEAOB), and the Public Company Accounting Oversight Board (PCAOB) in the United States.

The EDPB welcomes the CEAOB's efforts to address this matter in a coordinated manner by its members, with the setting up of a dedicated Taskforce in this respect and also appreciates your proposal to exchange with the CEAOB on this topic.

Regarding the two draft administrative arrangements for the two Member States you refer to in your e-mail, I would like to clarify that the EDPB has been following up informally on these two files. The competent Supervisory Authorities have not yet submitted the draft administrative arrangements to the consistency mechanism, pending their finalization and the steps that need to be taken first at national level. Apart from these two draft administrative arrangements, auditor oversight authorities of other Member States will also have to align their own arrangements with the PCAOB under the GDPR or should consider the need to enter into relevant arrangements with the PCAOB. For this reason, the intervention of the CEAOB as coordinator throughout this process will be needed in order to ensure the consistency of these arrangements.

The EDPB's International Transfers Subgroup (ITS) is available to hold an exchange to clarify any questions that you or your members may have regarding the EU data protection requirements related to the setting up of such administrative arrangements in light of the EDPB Guidelines 2/2020 on articles 46.2 (a) and 46.3 (b) relating to transfers of personal data between EEA and non-EEA public authorities. If the CEAOB and its members deem so appropriate and that it would be beneficial for its work ahead you could invite the PCAOB to such an exchange between the CEOB and the EDPB's ITS subgroup.

I suggest that your team liaises with the ITS subgroup coordinators regarding the organization and practical arrangements of a meeting by writing at the following address:  
[edpb-secretariat@edpb.europa.eu](mailto:edpb-secretariat@edpb.europa.eu).

Yours sincerely,



Andrea Jelinek

**Andrea Jelinek**  
Chair of the European Data Protection Board

rue Wiertz, 60  
1047 Brussels

Moritz Körner,  
Member of the European Parliament

Brussels, 16 June 2020

By email only

Ref: OUT2020-0061

Dear Mr Körner

Thank you for your letter of 23 January 2020 as regards the relevance of encryption bans in third countries for assessing the level of protection in accordance with the GDPR when personal data are transferred to countries where these bans exist.

Encryption (cryptography, more in general) is a technology, which, if implemented in the right way, provides for the effective protection of the security of personal data and is a building block for many other privacy-enhancing technologies. The GDPR mentions it explicitly as a possible technical measure to ensure a level of security appropriate to the risks for the rights and freedoms of natural persons and takes it explicitly into account in assessing certain compliance obligations.

Security ("integrity and confidentiality") is one of the principles relating to the processing of personal data<sup>1</sup>, which uniquely contributes to the compliance and protection of individuals' fundamental rights in all processing activities. Article 32 GDPR gives to encryption, together with pseudonymisation, the rank of a measure that, yet as appropriate, may not be neglected when identifying security protection measures.

As the Working Party 29 already highlighted<sup>2</sup>, the EDPB considers the availability of strong and trusted encryption as a "*necessity in the modern digital world*" and a technology contributing in "... *an irreplaceable way to our privacy and to the secure and safe functioning of our societies*". They state that encryption "... *must remain standardized, strong and efficient, which would no longer be the case if providers were compelled to include backdoors or provide master keys*".

Any ban on encryption or provisions weakening encryption would undermine the GDPR obligations on the concerned controllers and processors for an effective implementation of both data protection principles and the appropriate technical and organisational measures. Similar considerations apply to transfers to controllers or processors in any third countries adopting such bans or provisions.

Security measures are therefore specifically mentioned among the elements the European Commission must take into account when assessing the adequacy of the level of protection in a third

---

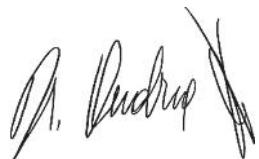
<sup>1</sup> See Article 5(1)(f) GDPR.

<sup>2</sup> "Article 29 WP Statement on encryption": [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=622229](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622229)

country.<sup>3</sup> In the absence of such a decision, transfers are subject to appropriate safeguards<sup>4</sup> or may be based on derogations<sup>5</sup>; in any case the security of the personal data has to be ensured at all times.

The EDPB is of the opinion that any encryption ban would seriously undermine compliance with the GDPR. More specifically, whatever the instrument used, it would represent a major obstacle in recognising a level of protection essentially equivalent to that ensured by the applicable data protection law in the EU, and would seriously question the ability of the concerned controllers and processors to comply with the security obligation of the regulation.

Yours sincerely,



Andrea Jelinek

<sup>3</sup> See Article 45(2)(a) GDPR.

<sup>4</sup> See Article 46 GDPR.

<sup>5</sup> See Article 49 GDPR.

Moritz Körner,  
Member of the European Parliament

Brussels, 16 June 2020

By e-mail only

Ref: Out-2020-0062

Dear Mr Körner,

Thank you for your letter of 23 January 2020 as regards your proposal on the possibility of establishing that all new laptops entering the EU market would need to be equipped with a physical camera cover based on article 25 GDPR.

The measures aimed at protecting and guaranteeing the rights and freedoms of natural persons must be established by the controller. Although manufacturers should be encouraged to take into account the right to data protection when developing and designing such products, services and applications, they are not responsible for the processing carried out with their products<sup>1</sup>. The GDPR does not provide for means to establish legal obligations on manufacturers, unless they also act as controllers or processors.

The GDPR does not specify any specific measure to fulfil the requirements of data protection by design and by default. Therefore, the controller shall choose the most appropriate measures according to the circumstances for the specific processing. As indicated in your letter, the physical camera cover is a tested, simple, cheap and efficient technology to prevent the camera from unduly collecting images. Nevertheless, there are other measures that could also be taken into consideration, *inter alia*, incorporating a physical on/off switch, or an easy way to deactivate the camera.

In addition, there are software solutions that can serve the same purpose and that give the control to the user. Nonetheless, the use of a software measure could present other associated risks, like bugs, introduction of unwanted “features” or the possibility of disabling the measure through remote access.

---

<sup>1</sup> See Recital 78 of the GDPR.

To summarize, the objective of the controller shall be to provide sufficient guarantees to implement appropriate technical and organisational measures in such manner that the processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject. The controller shall choose the most appropriate measures for each specific processing according to the circumstances and following a risk assessment, in compliance with the GDPR.

Yours sincerely,



Andrea Jelinek

Ailidh Callander  
Legal Officer  
Privacy International  
62 Britton Street  
London, EC1M 5UY  
United Kingdom

18 June 2020

Ref: OUT2020-0063

Dear Ms Callander,

I refer to your letter dated 30 May 2019.

Many thanks for bringing Privacy International's case study on the TrueCaller app to our attention. The relevant expert subgroups have now reviewed both the case study and your correspondence with TrueCaller. Information about your interest in the TrueCaller app has been forwarded to national supervisory authorities.

The role of the European Data Protection Board is to ensure the consistent application of the GDPR, whereas the competence to handle complaints and launch enforcements actions lies with the national supervisory authorities. Therefore, the European Data Protection Board lacks the competence to take an enforcement action or initiate an investigation regarding a specific company.

When complaints are lodged at national supervisory authorities, the various national authorities may consult and coordinate on the matter under the one-stop-shop mechanism provided for by the GDPR.

Please note that the European Data Protection Board will not be in a position to discuss or comment on pending procedures.

Yours sincerely,



Andrea Jelinek

Monique Goyens  
Director General, BEUC  
Ursula Pachl  
Deputy Director General, BEUC  
Rue d'Arlon 80 - B-1040 Brussels

18 June 2020

Ref: OUT2020-0064

Dear Ms. Goyens, Dear Ms. Pachl,

I refer to your letter dated 14 January 2020 regarding *Forbrukerrådet's* (the Norwegian Consumer Council's) "Out of Control" report, concerning consumers and the alleged privacy infringements of the adtech industry.

Thank you very much for bringing this important topic to our attention. We appreciate your efforts to put such a relevant issue on the agenda of different agencies and organisations across Europe.

The importance of the topic at hand is reflected in the EDPB Work Program 2019/2020, where we, *inter alia*, are working on Guidelines on Targeting of social media users.

The EDPB is not able to comment on ongoing investigations conducted by national supervisory authorities. We also lack the required competence to launch investigations, as this competence lies with the relevant national supervisory authorities.

However, please be assured that the topic of privacy in the adtech industry is assigned to the relevant EDPB Expert Subgroups. In addition, with regards to cross-border cases, the One-Stop-Shop mechanism in the GDPR ensures that the lead supervisory authority in a case cooperates and receives input from concerned supervisory authorities. The EDPB and its Expert Subgroups also serve as a useful forum for the national supervisory authorities to coordinate, cooperate and exchange experiences in ongoing cases – whether they are cross-border cases or not.

As you state in your letter, *Forbrukerrådet* has lodged formal complaints with the Norwegian supervisory authority. We are also aware that other supervisory authorities have received similar inquiries from their respective national consumer authorities. We are confident that the GDPR and EDPB cooperation mechanisms will serve as helpful tools for the national supervisory authorities in handling these cases, working together to ensure a uniform application of the GDPR in the EEA.

Thank you again for your letter.

Yours sincerely,



Andrea Jelinek

**Andrea Jelinek**  
Chair of the European Data Protection Board  
rue Wiertz, 60  
1047 Brussels



Ms Ďuriš Nicholsonová  
Member of the European Parliament

17.07.2020

by e-mail only

Ref: OUT-2020-0089

Dear Ms Ďuriš Nicholsonová,

Thank you very much for following up on the recent EDPB letter with regard to the need for common guidance on the application of the General Data Protection Regulation (GDPR), and other relevant legal instruments of the EU in matters of data protection, in the fight against the COVID-19 pandemics.

You now address the EDPB, asking additional questions on the use of contact tracing as part of a comprehensive approach to address the COVID-19 health related crisis. More specifically, your concerns span over four issues broadly related to potential discrepancies in the various measures envisaged in the Member States, the applicability of those measures in connection with the duration of the emergency, the implementation of DPIAs for contact tracing solutions and the use of similar technical tools to enforce social distancing where this requirement is in place.

Let me preliminarily clarify that the GDPR does not envisage the suspension of data protection principles and individuals' rights in case of emergencies; in fact, it explicitly mentions (rec. 46) the relevance of processing personal data for humanitarian purposes, including epidemics, within the framework of legal conditions such as the necessity to protect the vital interests of the data subject or of another natural person, or the performance of a task carried out in the public interest. Both are applicable legal bases for the processing, in compliance with art. 6(1)d and art. 6(1)e respectively. Also, the GDPR in art. 23 allows Member States to restrict, by way of a legislative measure, the scope of a number of specific obligations and rights when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society<sup>1</sup>. Similarly, the e-privacy Directive in art 15 allows Member States to adopt legislative measures to restrict the scope of the rights and obligations with respect to the processing of personal data in the electronic communication sector, for a limited number of purposes in the public interest and with the same caveat in terms of necessity and proportionality of the said legislative measures.

Regarding more specifically your questions, the EDPB is aware that multiple stakeholders believe a harmonized approach within the EU in contact tracing applications may help de-escalation of the epidemics. Its Members are monitoring the situation at national level, surveying both the legal instruments that are being enacted and the technical implementation of the contact tracing apps.

---

<sup>1</sup> The EDPB has recently adopted a statement on data subject rights restrictions in connection to the state of emergency in Member States (2 June 2020)

<https://edpb.europa.eu/our-work-tools/our-documents/ine/statement-restrictions-data-subject-rights-connection-state>

Further, the EDPB has very recently issued a statement on the issue of interoperability of contact tracing applications<sup>2</sup>.

As for your second question, it is very difficult to make any prediction on the duration of this emergency and to modulate the actions depending on the severity, or any potential new rise of the epidemics. Nevertheless, respect of the general principles of effectiveness, necessity, and proportionality remains paramount in all cases. The EDPB has repeatedly stated that the data processed in the context of contact tracing applications should be limited to the bare minimum when the implementation of such apps is useful, and that once such applications are not deemed anymore necessary for the original purpose, these systems should not remain in use, and as a general rule, the collected data should be erased or anonymised. Practically, this can be done also in an asynchronous way when “return to normal” is decided by the competent public authorities, with a procedure that terminates the collection of identifiers and activates the deletion of all collected data from all databases.

In your letter, you put forward the argument that having to go through a mandatory data protection impact assessment (DPIA) might delay the implementation of contact tracing applications at national level. The EDPB has clarified that the DPIA is a crucial step in addressing high risk situations as well as an integral part of the overall design of any technical solution<sup>3</sup>. The assessment of risks to individuals' rights and freedoms, and the strategies to mitigate those risks cannot be separated from the technical implementation: they jointly make up the privacy by design approach promoted by the GDPR. This is the norm, and the EDPB has provided criteria to arrange a DPIA<sup>4</sup> in many contexts that can be usefully considered by data controllers in this phase to enhance the efficiency and effectiveness of contact tracing solutions. National DPAs are also available as always to provide advice and guidance quickly and effectively, in the light of those common criteria but taking account of the specificities of the individual solutions.

Finally, you refer to Member States' possible intention to launch additional tracking applications for enforcing home quarantine or social distancing restrictions. To the knowledge of the EDPB, this is not the scope of the current contact tracing applications, which are only aimed at detecting potential contacts with COVID-19-positive persons in order to facilitate the delivery of the appropriate information to the concerned persons, and to increase the effectiveness of the subsequent health care procedures. Should other tools be developed at national level for those different enforcement purposes, they should be regulated in compliance with the EU and national data protection legal framework on the basis of a thorough legal and technical analysis and in line with the general data protection by design approach mentioned above.

---

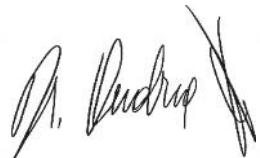
<sup>2</sup> [https://edpb.europa.eu/our-work-tools/our-documents/drugo/statement-data-protection-impact-interoperability-contact-tracing\\_en](https://edpb.europa.eu/our-work-tools/our-documents/drugo/statement-data-protection-impact-interoperability-contact-tracing_en)

<sup>3</sup> This DPIA may be performed in the context of the adoption of the legal basis used for the processing in line with Art 35 (10) GDPR.

<sup>4</sup> See WP29 guidelines (adopted by the EDPB) on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679

I would like to thank you for your continued interest in the work of the EDPB. The EDPB will continue to proactively monitor the situation and provide Guidance when necessary.

Yours sincerely,



Andrea Jelinek

Miguel de Serpa Soares

7 October 2020

Under-Secretary-General for Legal Affairs and United Nations Legal Counsel

United Nations

N.Y. 10017

United States

Ref: OUT2020-0109

Dear Mr. de Serpa Soares,

Thank you for the constructive discussion in Brussels last February and your follow-up letters of 26 February 2020 and of 14 May 2020, by which you also provided comments on the "Guidelines 2/2020" referred to as "Guidelines 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". These comments provide valuable input for the further work of the European Data Protection Board on these guidelines.

Let me note that in the "Non-Paper (point (3))" accompanying your letter of 26 February 2020, reference is made to the explanations given by the European Commission in its letter dating from 3 July 2018 on the privileges and immunities of international organisations. In its guidance<sup>1</sup>, the European Data Protection Board has also clarified that the application of the GDPR is without prejudice to the provisions of international law, such as the ones governing the privileges and immunities of international organisations. At the same time, this guidance highlights that entities subject to the GDPR that exchange personal data with international organisations have to comply with the GDPR, including its rules on international transfers (Chapter V of the GDPR).

As a preliminary observation, the European Data Protection Board notes that, indeed, pursuant to Article 45 GDPR, transfers from the EEA to a third country or an international organisation can take place where the third country or the international organisation ensures a level of protection considered adequate by the European Commission. Such a finding is based on a comprehensive assessment by the European Commission which takes into account a number of elements, e.g. the legal data protection framework of such a third country or international organisation as a whole, in order to determine if that third country or international organisation ensures a level of protection essentially equivalent to that ensured within the European Union. Whilst this assessment focuses on different elements, such as the substantive privacy rules and individual rights provided by the legal system of the third country or international organisation, as well as their effective implementation, the main purpose of this assessment is, *inter alia*, to verify that effective independent data protection supervision and enforceable rights and effective legal remedies for data subjects are provided by the

---

<sup>1</sup> Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), p.23.

third country or international organisation<sup>2</sup>, it does not mean that, in practice, those have to be provided in the same way as they are in under the GDPR.

The European Data Protection Board has already issued guidance on several other instruments for international transfers, which is also relevant for data transfers to international organisations. For example, transfers to United Nations System Organisations from EU public bodies subject to the GDPR can be performed relying in particular on a legally binding and enforceable instrument under Article 46 (2) (a) or on administrative arrangements under Article 46 (3) (b) of the GDPR. On this issue, the EDPB has, as you know, issued draft Guidelines<sup>3</sup>, which can provide useful clarifications also having regard to transfers to United Nations organisations. These guidelines, for instance, recognise that certain safeguards, e.g. ensuring judicial redress or independent oversight through external bodies, may not be available for international organisations and provide examples of possible alternative mechanisms that could be developed.<sup>4</sup> The guidelines will now be finalised following the public consultation.

Useful clarifications on international transfers have also been provided by the European Data Protection Board in the Guidelines on derogations pursuant to Article 49 of the GDPR<sup>5</sup>, which clarify e.g. when personal data may be transferred in specific situations if necessary for important reasons of public interest.<sup>6</sup> This may, for instance, be the case if there is an international agreement to which the EU or its Member States are a party that recognises a certain objective and provides for international cooperation to foster that objective.

With respect to exchanges of data with service providers in the EU, to which your letter specifically refers, I would also like to point to the clarifications already provided by the European Data Protection Board. In particular, the guidelines on the territorial scope of the GDPR clarify the specific (and limited) obligations of service providers established in the EU that carry out processing on behalf of an entity that is not subject to the GDPR.<sup>7</sup>

At the same time, I understand that certain questions remain. I would, therefore, like to inform you that the European Data Protection Board will explore ways to further clarify how the rules on international transfers under the GDPR apply when personal data is transferred to international organisations. Please note that this may require some time due to the judgment of the Court of Justice of the European Union in case C-311/18 (*Schrems II*) issued on 16 July 2020. As you have probably

---

<sup>2</sup> See recital 104 GDPR.

<sup>3</sup> 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.

<sup>4</sup> 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 - version for public consultation, p. 11 (para 47) referring to judicial redress and p.12 (para 57) referring to oversight mechanism.

<sup>5</sup> Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, as adopted by the European Data Protection Board on 25 May 2018.

<sup>6</sup> Guidelines 2/2018 on derogations of Article 49, p. 10 et. seq.

<sup>7</sup> Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), p.12 et seq.

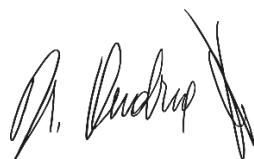
noted, the European Data Protection Board has started working on the follow-up of this judgment<sup>8</sup>, relevant for any transfer question, and will continue to do so in the upcoming months.

The Board is ready to engage with international organisations in this context.

The regular workshops with international organisations organised by the European Data Protection Supervisor, which next edition is scheduled for 8-9 October 2020, seem to be the appropriate venue to continue the discussions. United Nations representatives already took part to these workshops in the past and have already been invited to this edition.

The European Data Protection Board remains available to further engage with the United Nations System Organisations on our shared mission of protecting international human rights, including the right to privacy.

Yours sincerely,



Andrea Jelinek

---

<sup>8</sup> See in particular FAQs on the judgment of the CJEU in case C-311/18, adopted on 23 July 2020.

Sophie in't Veld  
Member of the European Parliament

By email only

3 December 2020

Ref: OUT2020-0132

Dear Ms in't Veld,

Thank you very much for your letter dated 12 July 2019, in which you ask if the EDPB intends to publish the full and unredacted minutes of the EDPB plenary sessions.

I am pleased to inform you that on 14 September 2020, the EDPB adopted internal guidance<sup>1</sup>, and consequently, the minutes of that plenary meeting have been published on the EDPB website. The minutes of future and previous plenary meetings will be published in due course.

Yours sincerely,



Andrea Jelinek

---

<sup>1</sup> [https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_guidance\\_202009\\_plenaryminutes\\_en.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidance_202009_plenaryminutes_en.pdf)

Sophie in 't Veld

Member of the European Parliament

By email only

Ref: OUT2020-0004

Subject: Your letter to the EDPB of 31 July 2019

Dear Mrs in 't Veld,

I would like to thank you for your letter dated the 31<sup>st</sup> of July 2019 concerning the appropriateness of the GDPR as a legal framework to protect citizens from unfair algorithms, including the question as to whether EDPB would find it relevant to express its intention to issue guidelines on this topic.

Please find below an answer for each of the questions you raised. Please be reassured that the EDPB takes this topic very seriously and will continue to reflect on any topic that might have an impact on the right to data protection of the citizens.

Yours sincerely,



Andrea Jelinek

## Does the EDPB consider that the GDPR can sufficiently protect citizens from unfair algorithms?

The EDPB is of the opinion that the GDPR is a robust legal framework to protect citizens' right to data protection. As you know, the GDPR is built in a technologically neutral manner in order to be able to face any technological change or evolution. As per its competence, the EDPB can only answer the question from the data protection perspective. It is, however, well aware that the issue of unfair algorithms may also have consequences in other areas, such as in consumer protection, antidiscrimination and competition law. Members of the EDPB have therefore continuously engaged with other relevant regulatory authorities in their member states and at EU level.

Any processing of personal data through an algorithm falls within the scope of the GDPR. This means that the GDPR covers the creation of and use of most algorithms. Thanks to - *inter alia* - the risk based approach, the data minimisation principle and the requirement of data protection by design and by default, the current legal framework addresses many of the potential risks and challenges associated with the processing of personal data through algorithms.

Algorithms can result unfair or even discriminatory outcomes for many reasons that need to be addressed separately because each of them may require specific levels of protection for the involved individuals. For instance, as can be the case with personalised services, discrimination can be an intentional choice of the creator of the algorithm or of the decision maker.<sup>1</sup> Secondly, some datasets that are collected in our current society may contain signs of biased, unjust, unfair or even discriminatory beliefs and behaviour, or simply reflect the habits of a majority of individuals, whose preferences may be perceived as unfair and discriminatory for the minority. Hence, when algorithms are trained on the basis of such biased data or on the basis of mismatches between majorities and minorities, the resulting algorithm will reflect this bias or mismatch.<sup>2</sup> Finally, discrimination may even come as an unintentional side effect of the design or use of the algorithm. Some of these sources of discrimination have to do with human intentions and require specific behavioural or ethical safeguards, others have to do with the way data, sometimes personal data, is processed.

In addition to the risk of unfair treatment, algorithms present two other challenges from a data protection perspective, which are inherent to the technology. Firstly, there is the incentive for processing large amounts of data: the common assumption is that the more data is used to train algorithms, the more accurate they become at predicting what they were trained to do. Apart from

---

<sup>1</sup> Gary S. Becker in "The economics of discrimination" (Milton Friedman ed., 2nd ed. 1971).

<sup>2</sup> For a discussion on the risks of discrimination by algorithms see 'Discrimination, artificial intelligence, and algorithmic decision-making', Prof. Frederik Zuiderveen, University of Amsterdam, Council of Europe 2018, available at <https://www.coe.int/en/web/european-commission-against-racism-and-intolerance/studies>.

questioning the general validity of this assumption<sup>3</sup>, this “data maximization” approach creates an incentive for large and possibly unlawful data collection and further processing of data. Secondly, algorithms are becoming more and more complex, which makes them less transparent. This lack of transparency is caused by the fact that the inner workings of the algorithms are simply very difficult to understand or explain (“black box”). This can lead to a lack of transparency towards the data subject whose data is processed by the algorithm and a loss of human autonomy for those working with algorithms.

While the GDPR is applicable in its entirety to all processing of personal data, the EDPB would like to highlight specific provisions that can play an important part in addressing the potential risks arising from the use of algorithms. The general principles laid out in Art. 5 GDPR, specifically lawfulness, fairness and transparency, accuracy, data minimisation and purpose limitation govern the processing of personal data, both when creating<sup>4</sup> and using algorithms.

The principle of transparency, further specified in articles Art. 12-14 GDPR, requires that controllers take appropriate measures in order to keep the data subjects informed about how their data is being used. This needs to be done in a concise, transparent, intelligible and easily accessible way.<sup>5</sup> These provisions require anyone using an algorithm for automatic decision-making, to inform data subjects of the existence of this process and provide meaningful information about its logic, as well as the significance and envisaged consequences.<sup>6</sup> Furthermore, Recital 60 explicitly states that the data subject should be informed of the existence of profiling and the consequences of such profiling. Transparency is about enabling data subjects to understand and to make use of their rights in Art. 15 to 22 GDPR, if necessary. Further, it is about controllers’ obligation to ensure that data subjects are not adversely impacted, including by unintentional consequences of algorithmic decisions (principle of accountability).

Furthermore, on the basis of Art. 25 GDPR, data controllers have to ensure data protection by design and by default, meaning they need to put in place appropriate measures that are designed to

---

<sup>3</sup> E Junqué de Fortuny, D Martens, F Provost, in “Predictive Modeling with Big Data: Is Bigger Really Better?” *Big Data*, 2013, vol. 1, no. 4, pp. 215–226.

<sup>4</sup> This can be achieved by data protection by design and by default in the creation of algorithms: EDPB ‘Guidelines 4/2019 on Article 25 Data Protection by Design and by Default’. Version 1.0, 13 November 2019. [https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design\\_en](https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en).

<sup>5</sup> Recital 39, Article art. 5(1) and art. 12-14 GDPR; for further elaboration on the principle of transparency, see the Article 29 Working Party. “Guidelines on transparency under Regulation 2016/679”. WP260 rev.01, 11 April 2018 - endorsed by the EDPB. [https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc\\_id=51025](https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025).

<sup>6</sup> Articles 13(2)(f), 14(2)(g) GDPR.

effectively implement the aforementioned data protection principles, protect the rights and freedoms of natural persons and integrate necessary safeguards, when deciding to use or when training an algorithm. This requires a data protection oriented approach when developing the technology in the various steps of development, selection and use of algorithms.<sup>7</sup>

In addition, the principle of accountability requires that the controllers ensure compliance with the GDPR and are able to demonstrate this compliance.<sup>8</sup> This means controllers are obliged to consider all the potential risks that the use or creation of the specific algorithm can potentially pose to the rights and freedoms of natural persons and, if necessary, take measures to address these risks. While Art. 24 GDPR primarily concerns the rights to data protection and privacy, it may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, and the rights to liberty, conscience and religion.<sup>9</sup>

The use or development of an algorithm can trigger the obligation to carry out a Data Protection Impact Assessment (DPIA) (Art. 35 GDPR) prior to any processing taking place. If the outcome of the DPIA indicates that the processing would, in the absence of measures, result in a high risk, the controller will have to consult the relevant supervisory authority prior to the processing.<sup>10</sup> The outcome of the assessment can also be that the controller will have to refrain from using a specific algorithm, or parts of it, if the risks to the rights of data subjects and other persons cannot be sufficiently mitigated. All the processing activities and the measures taken to ensure compliance as described in the DPIA need to be included in the records of processing activities, which can be viewed by the supervisory authorities as part of its investigative powers.<sup>11</sup>

Lastly, the GDPR contains specific provisions concerning automatic decision-making. Art. 22 GDPR prohibits any decision-making based solely on automatic processing, if such a decision '*produces legal effects concerning [the data subject] or similarly significantly affects [the data subject]*'.<sup>12</sup> This means

---

<sup>7</sup> Article 25 GDPR, EDPB ‘Guidelines 4/2019 on Article 25 Data Protection by Design and by Default’. Version 1.0, 13 November 2019. [https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design\\_en](https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en); see specifically the subsection on “fairness” in section 3.

<sup>8</sup>Article 24 GDPR and art. 5(2) GDPR.

<sup>9</sup> Art. 24 and Art. 35 GDPR; Article 29 Working Party “Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679”. WP 248 rev.01, 4 2017 - endorsed by the EDPB. [https://ec.europa.eu/newsroom/document.cfm?doc\\_id=47711](https://ec.europa.eu/newsroom/document.cfm?doc_id=47711).

<sup>10</sup> Article 36 GDPR.

<sup>11</sup> Article 24 and Article 58 GDPR.

<sup>12</sup> Art. 22(1) GDPR. This prohibition has limited exceptions listed in Article 22(2) GDPR. See for more specific guidance on Article 22: Article 29 Working Party “Guidelines on Automated individual decision-

that in practice it will often not be possible to rely solely on the outcome of an algorithm for sensitive decision-making. Furthermore, Art. 22 requires the controller to implement suitable measures to safeguard the data subject's rights and freedoms and its legitimate interests, which has to include the right to obtain human intervention.<sup>13</sup> This human intervention has to be qualified, capable of discovering and recovering unfair outcomes or discriminations, as the EDPB has recently pointed out in its guidelines on data protection by design and by default.<sup>14</sup>

**Does the EDPB consider that enforcement of the GDPR in the context of algorithms is sufficient and effective, or does it consider that additional and specific legislation is necessary to better protect citizens against discriminatory algorithms, and to provide more transparency on the functioning of algorithms?**

**Furthermore, will the EDPB issue guidelines on what it considers a fair algorithm?**

Considering the already extensive existing legal framework the EDPB considers additional legislation in the area of data protection aimed at a specific technology as premature at this time. Rather our focus at this time lies on the development of existing norms, specifically the requirements of transparency, accountability and the DPIAs in the context of machine learning algorithms. In the future, this may lead to the development of guidelines.

Taking into account that the use of 'unfair' algorithms may have consequences outside of the area of data protection, the EDPB believes that in order to protect individuals from unfair or discriminatory outcomes of algorithms an interdisciplinary approach is needed. The current legal framework for data protection does however offer many options for effective supervision and enforcement on the aforementioned aspects of fairness and transparency, and individuals' rights, granting control over their personal data by data protection authorities. This enforcement can take many forms, including, but not limited to:

- actively informing the public regarding their rights;
- engaging with stakeholders;
- informing and guiding organisations;
- assessing prior consultations and;
- carrying out investigations, which may lead to enforcement actions.

---

making and Profiling for the purposes of Regulation 2016/679" WP 251 rev.01, As last Revised and Adopted on 6 February 2018 – endorsed by the EDPB.  
[https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=612053](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053).

<sup>13</sup> Art. 22(3) GDPR.

<sup>14</sup> EDPB 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default". Version 1.0, 13 November 2019. [https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design\\_en](https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en).

Several authorities have received requests for prior consultations, informal requests for advice from organisations that include algorithmic technology and some have issued and contributed to guidance.<sup>15</sup> At the same time, the EDPB recognises that ensuring effective enforcement of the existing obligations under the GDPR in the context of this fast developing technology will continue to require considerable and continuous investment in up-to date expertise and sufficient resources in the coming years.

---

<sup>15</sup> See <https://www.datatilsynet.no/en/regulations-and-tools/reports-on-specific-subjects/ai-and-privacy/> (Norwegian Data Protection Authority); <https://ico.org.uk/about-the-ico/news-and-events/ai-auditing-framework/> (UK Data Protection Authority); <https://www.cnil.fr/en/algorithms-and-artificial-intelligence-cnils-report-ethical-issues> (French Data Protection Authority) [https://www.bmjjv.de/DE/Themen/FokusThemen/Datenethikkommission/Datenethikkommission\\_E\\_N\\_node.html](https://www.bmjjv.de/DE/Themen/FokusThemen/Datenethikkommission/Datenethikkommission_E_N_node.html) (Germany's Federal Date Ethics Committee (Datenethikkommission)) ; [https://www.datenschutz-berlin.de/fileadmin/user\\_upload/pdf/publikationen/working-paper/2018/2018-IWGDPT-Working\\_Paper\\_Artificial\\_Intelligence.pdf](https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2018/2018-IWGDPT-Working_Paper_Artificial_Intelligence.pdf) (International Working Group on Data Protection in Telecommunications); [http://globalprivacyassembly.org/wp-content/uploads/2018/10/20180922\\_ICDPPC-40th\\_AI-Declaration\\_ADOPTED.pdf](http://globalprivacyassembly.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf) (International Conference of Data Protection and Privacy Commissioners).

Brussels, 29 January 2020

**Alexander Seger**

Head of the Cybercrime Division, Council of Europe

**Members of the Cybercrime Convention Committee of the Council of Europe**

By email only

Ref: OUT2020-0005

Dear Mr Seger,

Dear Members of the Cybercrime Convention Committee,

As several members of the European Data Protection Board (EDPB) had the opportunity to participate to the Octopus conference which took place in Strasbourg on 20-22 November 2019, I would like to extend my thanks to the Cybercrime Convention Committee (T-CY) for the organisation of this event, allowing for a fruitful exchange on issues related to international cooperation in combating cybercrime, in particular the Second Additional Protocol to the Budapest Convention, and the importance of data protection safeguards in this context.

We are particularly grateful that the EDPB contribution to the consultation on the Second Additional Protocol<sup>1</sup> has been made available to participants and that members of the EDPB were able to present our main observations and recommendations. EDPB members who attended the Octopus Conference welcomed the opportunity to further discuss the provisional text of provisions on direct disclosure of subscriber information and on the giving effect of orders for expedited production of data. We understand, however, that discussions were limited to the perimeter of these provisional texts and could not fully extend to other provisions, such as the ones related to data protection, which are still being negotiated.

The drafting of the Second Additional Protocol is sensitive from a data protection perspective, as all the envisaged new procedures involve the collection of personal data, including not only subscriber but also traffic data, on the basis of orders from another jurisdiction. For the EU, but also most of the other Parties to the Budapest Convention that have rules on international data transfers (e.g. as Parties to the Council of Europe Convention 108), this makes it indispensable to ensure that strong safeguards providing a high level of data protection become an integral part of the final text, applicable to all Parties. The EDPB contribution to the consultation on the Additional Protocol includes a detailed reference to specific safeguards, which might be further developed in the future once more information on the status and content of the discussions becomes available. As already stated in the contribution, the EDPB considers it essential that the provisional text submitted to public consultation is complemented by dedicated provisions on data protection safeguards, which must then be assessed together in order to ensure that the draft Additional Protocol translates into a sustainable arrangement, in compliance with EU primary and secondary law.

---

<sup>1</sup> EDPB contribution to the consultation on a draft second additional protocol to the Council of Europe Convention on Cybercrime - 13/11/2019.

The EDPB considers it essential that the ongoing discussions for the drafting of the Additional Protocol are carried out with a high level of transparency and ultimately lead to the establishment of a modernised instrument for the exchange of personal data with third countries for fighting cybercrime that is both consistent with the Council of Europe acquis, in particular Convention 108, and fully compatible with the EU Treaties and the Charter of Fundamental Rights. We therefore hope that the T-CY will swiftly reach a provisional agreement in drafting such data protection safeguards and that a dedicated consultation process will be carried out prior to the finalisation of the draft Second Additional Protocol.

The EDPB intends to closely follow the advancement of the negotiations while remaining available and committed to provide a constructive and objective contribution with a view to ensure that data protection considerations are duly taken into account in the overall drafting process of the Second Additional Protocol to the Budapest Convention.

Yours sincerely,



Andrea Jelinek

**Andrea Jelinek**

Chair of the European Data Protection Board

rue Wiertz, 60  
1047 Brussels

Anna-Michelle Asimakopoulou,  
Member of the European Parliament

Brussels, 25 January 2021

By e-mail only

Ref: OUT2021-0002

Dear Ms Asimakopoulou,

Thank you for your letter of 19 October 2020 regarding the developments in relation to ICANN/WHOIS. The EDPB is aware of the importance of this matter and has considered the issues related to the development of a GDPR-compliant WHOIS model on previous occasions, including in its letter of 5 July 2018<sup>1</sup>.

In this context, the EDPB recalls that the GDPR provides for the so-called 'One-Stop-Shop' mechanism, which stipulates that for any cross-border processing of personal data the data protection authority of the main or of the single establishment of the data controller in the EEA acts as the competent authority, which supervises the processing activities of that controller.

Therefore, the EDPB underlines that the Belgian data protection authority is the competent authority to supervise ICANN's processing activities in relation to their compliance with the GDPR<sup>2</sup>.

The EDPB is confident that the Belgian data protection authority is fulfilling its tasks and exercising its powers in accordance with the GDPR. The EDPB recalls that the cooperation and consistency mechanism as provided in the GDPR enables the national supervisory authorities to work together in order to contribute to the consistent application of the GDPR.

The role of the EDPB is to ensure the consistent application of the GDPR, whereas the competence to monitor processing activities of data controllers and to advise them regarding their obligations under the GDPR lies with national supervisory authorities. In accordance with Article 64 (2) GDPR, the EDPB may be requested to examine any matter of general application or producing effects in more than one Member State, however only supervisory authorities, the Chair of the Board or the European Commission can submit such a request to the EDPB on the basis of Article 64 (2) GDPR.

Please note that the general guidance by the EDPB on allocation of the processing roles in accordance with the GDPR has been provided in the EDPB Guidelines 07/2020 on the concepts of controller and

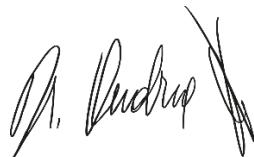
---

<sup>1</sup> EDPB letter to the President and CEO of the Board of Directors of ICANN of 5 July 2018, available at: [https://edpb.europa.eu/sites/edpb/files/files/file1/icann\\_letter\\_en.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/icann_letter_en.pdf); See also the EDPB endorsed the statement of the WP29 on ICANN/WHOIS: [https://edpb.europa.eu/news/news/2018/european-data-protection-board-endorsed-statement-wp29-icannwhois\\_en](https://edpb.europa.eu/news/news/2018/european-data-protection-board-endorsed-statement-wp29-icannwhois_en)

<sup>2</sup> In this respect we refer to the letter of the Belgian supervisory authority to the President and CEO of the Board of Directors of ICANN of 9 August 2018, available at: <https://www.icann.org/en/system/files/correspondence/debeuckelaere-to-marby-26sep18-en.pdf>

processor in the GDPR<sup>3</sup>. Various stakeholders, including ICANN, submitted their views and questions during the public consultation that ended on 19 October 2020<sup>4</sup>. The EDPB will now continue its work in finalising these guidelines taking into account the feedback received during the public consultation.

Yours sincerely,



Andrea Jelinek

---

<sup>3</sup> EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, available at [https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices\\_en](https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en)

<sup>4</sup> The public comments of ICANN are available at:

[https://edpb.europa.eu/sites/edpb/files/webform/public\\_consultation\\_reply/controllerprocessorcomments.pdf](https://edpb.europa.eu/sites/edpb/files/webform/public_consultation_reply/controllerprocessorcomments.pdf)

# Letters



Miguel de Serpa Soares  
Under-Secretary-General for Legal Affairs and United Nations Legal Counsel  
United Nations N.Y. 10017  
United States

*Sent by email only*

Brussels, 18 November 2021  
Ref: OUT2021-00156

Dear Mr. de Serpa Soares,

Thank you for your letter of 15 July 2021, by which you refer to the ongoing dialogue between the European Data Protection Board (“the Board” or the “EDPB”) and the United Nations on data protection.

I would first of all like to thank you and the representatives of the United Nations System Organisations for the active participation in the Task Force on transfers to international organisations established by the European Data Protection Supervisor (the ‘Task Force’).

I understand that the work of this Task Force has indeed been very useful to allow its members to informally provide comments on various issues relating to transfers to international organisations, including on possible provisions for agreements or administrative arrangements. I am therefore pleased to read that representatives of several United Nations System Organisations will continue attending the Task Force.

As a consequence, and as I already indicated in my previous letter from 19 May 2021, the work carried out in this Task Force will not in any way replace any formal procedure set out in the GDPR.

Furthermore, I take the utmost account of your suggestion that the EDPB should consider addressing the situation of all transfers to United Nations System Organisations in a specific set of guidelines.

Lastly, I would like to renew the Board’s commitment to engage further with the United Nations System Organisations on the shared mission of protecting human rights, including the right to privacy.

Yours sincerely,



Andrea Jelinek



**Andrea Jelinek**  
Chair of the European Data Protection Board  
rue Wiertz, 60  
1047 Brussels

# Letters



Miguel de Serpa Soares  
Under-Secretary-General for Legal Affairs and United Nations Legal Counsel  
United Nations N.Y. 10017  
United States

***Sent by email only***

Brussels, 19 May 2021  
Ref: OUT2021-0086

Dear Mr. de Serpa Soares,

Thank you for your letter of 24 February 2021, by which you refer to the ongoing dialogue between the European Data Protection Board (“the Board” or the “EDPB”) and the United Nations on data protection.

The Board fully recognises the importance of the tasks and missions of international organisations in general and of the United Nations in particular, and of the specificities of such organisations, notably in the light of their privileges and immunities.

In this respect, the Board welcomes that the United Nations consider the final version of the Guidelines<sup>1</sup> on Article 46(2)(a) and 46(3)(b) of Regulation (EU) 2016/679 (“the GDPR”)<sup>2</sup> as providing useful clarifications.

These Guidelines should provide a general basis to interested parties, including international organisations, for the development of binding agreements or non-binding administrative arrangements depending on the case at hand or as a guidance for the safeguards to be provided for in different transfer tools which practical work on actual solutions may help identify.

Taking the above into account, in our reply letter of 7 October 2020, the Board expressed its commitment to engage with international organisations in this context and indicated the regular

---

<sup>1</sup> 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, [https://edpb.europa.eu/our-work-tools/our-documents/guidelines-22020-articles-46-2-and-46-3-b-regulation\\_en](https://edpb.europa.eu/our-work-tools/our-documents/guidelines-22020-articles-46-2-and-46-3-b-regulation_en).

<sup>2</sup> 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), L119 of 4.5.2016.

workshops with international organisations organised by the European Data Protection Supervisor ("the EDPS") as one possible appropriate venue to continue those discussions.

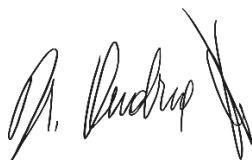
A workshop, held on 8 and 9 October 2020<sup>3</sup>, included a session dedicated to international transfers of personal data to international organisations, which provided an opportunity for an insightful and productive first exchange of ideas and information.

As a follow-up to this session, I wish to inform you that the EDPS has created a dedicated Task Force, whose first meeting took place on 14 April 2021 and to which several international organisations participated, together with some national supervisory authorities and the European Commission. The objective of this Task Force is precisely to further discuss- informally and without in any way replacing the formal procedures set out in the GDPR - how the rules on international transfers under the GDPR may apply when personal data is transferred to international organisations. Another meeting to discuss in more details the specific question of transfers from public entities to international organisations is already scheduled on 25 May 2021. We welcomed the participation of United Nations representatives to the first meeting of the Task Force and count on their continued participation to benefit from their valuable input to this Task Force on behalf of the United Nations System Organizations. Should your other colleagues be willing to participate to the work of such taskforce, please inform directly the EDPS ([POLICY-CONSULT@edps.europa.eu](mailto:POLICY-CONSULT@edps.europa.eu)).

I also look forward to receiving information on the update and strengthening of the data protection framework by the United Nations System Organizations you refer to in your letter and assure you that it will be considered with the utmost attention.

Lastly, I would like to renew the Board's commitment to further engage with the United Nations System Organizations on developing concrete transfer tools and in general on the shared mission of protecting human rights, including the right to privacy.

Yours sincerely,



Andrea Jelinek

---

<sup>3</sup> EDPS, Online Workshop: Data Protection within International Organisations 2020, 8 October 2020, [https://edps.europa.eu/data-protection/our-work/publications/events/online-workshop-data-protection-within-international\\_en](https://edps.europa.eu/data-protection/our-work/publications/events/online-workshop-data-protection-within-international_en).

Sophie in't Veld MEP

European Parliament  
Rue Wiertz 60  
B-1047 Brussels  
Belgium  
*by e-mail only*

Brussels, 07 July 2021  
Ref: OUT2021-0119

Dear Ms in 't Veld,

I would like to thank you for your letter of 28 May 2021 regarding the EDPB's statement 04/2021 on international agreements including transfers and for the questions raised.

As highlighted in the abovementioned statement, the EDPB deems that, in order to ensure that the level of protection of natural persons guaranteed by the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED) is not undermined when personal data is transferred outside the Union, consideration should be given to the aim of bringing international agreements involving the transfer of personal data to third countries or international organisations (also those related to FATCA) in line with the GDPR and LED requirements for data transfers where this is not yet the case.

Indeed, based on Article 96 of the GDPR and Article 61 of the Law Enforcement Directive, such agreements concluded prior to 24 May 2016 or 6 May 2016 and which comply with Union law as applicable prior to that date, shall remain in force until amended, replaced or revoked. Therefore, the EDPB considered such a statement as a useful reminder and invitation for Member States to review such agreements, where needed, and align them with the current European data protection legal framework.

Beforehand, the EDPB has adopted 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 in December 2020. These Guidelines set forth the standard regarding safeguards to be included in legally binding instruments or administrative arrangements between public bodies and are aimed at ensuring a consistent application of the GDPR in all Member States in line with the competences of the EDPB.

Against this background, I would like to stress again that the EDPB does not have the same competences, tasks and powers as national supervisory authorities (SAs) and, therefore, it is up to the latter to monitor and enforce, where necessary, the protection of personal data of data subjects within their jurisdiction. Also to this aim, the above mentioned statement clarifies that national SAs, are available to assist Member States in this exercise, keeping in mind however that Article 46(2). (a) GDPR does not refer to the need for the competent SA to authorise such kind of agreements.

In fact, one SA has received a complaint regarding the law applicable to the national intergovernmental agreement transposing FATCA and some SAs have already started discussions with their relevant Ministries regarding the review of such international agreements and the safeguards to be included in the new ones they are planning to conclude which is a long process. These bilateral discussions will take into consideration the abovementioned EDPB Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 so as to ensure that consistent safeguards will be inserted in the reviewed agreements and the new ones that will be adopted.

Yours sincerely,



Andrea Jelinek

# Letters



Mr Emmanuel Moulin,  
Mr Philippe Léglise-Costa  
Council of the European Union

***Sent by e-mail only***

Brussels, 12 May 2022

Ref: OUT2022-0030

Dear Sir,

This letter follows up on the adoption by the European Commission (“the EC”), of a legislative package of four legislative proposals (the “AML legislative proposals”) on 20 July 2021, aiming at strengthening the EU’s actions on anti-money laundering and countering the financing of terrorism (“AML/CFT”).

The legislative package includes a Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (“the Proposal for a Regulation applying to the private sector”)<sup>1</sup> and a Proposal for a Regulation of the European Parliament and of the Council establishing the European Authority for Countering Money Laundering and Financing of Terrorism (“the Proposal for a Regulation establishing AMLA”).<sup>2</sup>

The EDPB draws the attention of the European Institutions to the important data protection issues raised by the implementation of the AML/CFT obligations, as provided by the AML legislative proposals. Obligated entities are required to process personal data which allow to draw intimate inferences about individuals and which can notably lead to the exclusion of legal and natural persons from a right and/or a service (for instance, a banking service). It is therefore crucial that AML legislative proposals are in line with the General Data Protection Regulation (“the GDPR”).

---

<sup>1</sup> COM(2021) 420 final.

<sup>2</sup> COM (2021) 421 final.

The AML legislative package also includes a Proposal for a Directive of the European Parliament and of the Council on the mechanisms for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing, and a Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets.

**Andrea Jelinek**  
Chair of the European Data Protection Board

rue Wiertz, 60  
1047 Brussels

The EDPB also underlines that ensuring a better consistency between the AML legislative proposals and GDPR principles, such as the accuracy principle or the data minimisation principle, would improve the efficiency of the implementation of the AML/CFT legal framework.

To better achieve this consistency, the EDPB calls on the EU institutions to involve the EDPB in the discussions on the AML legislative proposals and suggests some crucial modifications having regard in particular to the Proposal for a Regulation applying to the private sector and the Proposal for a Regulation establishing AMLA.

This letter partly reiterates concerns expressed by the EDPB in its Statement published in December 2020<sup>3</sup>, in a letter addressed to the EC in May 2021<sup>4</sup>, as well as in the EDPS Opinion.<sup>5</sup> Indeed, the AML legislative proposals only partially implement the recommendations issued by the EDPB in 2020 and 2021. For instance, the EDPB notes that the EC has included, as requested by the EDPB, specific provisions on the processing of special categories of data<sup>6</sup> as well as on the processing of personal data relating to criminal convictions and offences<sup>7</sup> in the AML legislative proposals. However, the EDPB considers that the AML legislative proposals should provide for additional safeguards in relation to the processing of these personal data to ensure in particular compatibility with Articles 9 and 10 GDPR. Moreover, the AML legislative proposals do not provide specific rules in relation to the sources to be used by obliged entities for gathering information, and in relation to information provided by data service providers of so-called “watchlists”.

Without further amendments, the EDPB is of the view that the AML legislative proposals would have a disproportionate negative impact to the rights and freedoms of individuals and would lead to significant legal uncertainty. The EDPB would therefore like to highlight the following safeguards to be included in the AML legislative proposals.

### **1. Consultation of the EDPB in the context of the drafting and adoption of regulatory technical standards, guidelines and recommendations.**

The EDPB notes that regulatory technical standards (RTS), guidelines and recommendations to be developed and adopted by AMLA or the EC would, in practice, provide the core of the standardized AML/CFT rules.<sup>8</sup>

Indeed, pursuant to the AML legislative proposals, the RTS shall specify, notably, the information to be collected for the purpose of performing standard, simplified and enhanced customer due diligence<sup>9</sup>. Moreover, AMLA shall issue guidelines on ongoing monitoring of a business relationship and on the monitoring of the transactions carried out in the context of such relationship<sup>10</sup>. In addition,

---

<sup>3</sup> EDPB Statement on the protection of personal data processed in relation with the prevention of money laundering and terrorist financing, 15 December 2020.

<sup>4</sup> EDPB letter to the European Commission on the protection of personal data in the AML-CFT legislative proposals, 19 May 2021.

<sup>5</sup> EDPS Opinion 12/2021 on the anti-money laundering and countering the financing of terrorism (AML/CFT) package of legislative proposals.

<sup>6</sup> Special categories of data are defined in Article 9 GDPR.

<sup>7</sup> Processing of personal data relating to criminal convictions and offences is regulated under Article 10 GDPR.

<sup>8</sup> The Proposal for a regulation establishing AMLA, under Article 38, lays down that AMLA develops draft regulatory technical standards (RTS) and submits them to the EC for adoption. The RTS shall be adopted by the EC by means of delegated acts pursuant to Article 290 TFEU.

<sup>9</sup> Article 22 of the Proposal for a Regulation applying to the private sector

<sup>10</sup> Article 21(4) of the Proposal for a Regulation applying to the private sector  
Andrea Jelinek  
Chair of the European Data Protection Board

the EC shall issue recommendations to Member States on specific rules and criteria to identify the beneficial owners of legal entities other than corporate entities.<sup>11</sup>

First of all, the EDPB considers that the categories of personal data to be processed by obliged entities and additional rules that might impact their processing should not be specified in the RTS, guidelines, and recommendations, but rather be identified directly in the AML legislative proposals.

Furthermore, in accordance with its duty to ensure a consistent application of the GDPR<sup>12</sup>, the EDPB considers that its involvement in the development of RTS, guidelines and recommendations is essential to reach a common understanding between the concerned national data protection authorities, the AMLA and the EC, to clarify the interplay of the AML CFT legal framework with the GDPR, and thus to provide legal certainty to obliged entities.

Against this background, the EDPB notes that, while Recital 58 of the Proposal for a Regulation establishing AMLA provides that the AMLA shall “closely cooperate” with the EDPB, when “developing any instruments” or “taking any decisions” having a “significant impact on the protection of personal data”, the legal text of the Proposal only includes this obligation to cooperate in relation to guidelines and recommendations, without referring to RTS<sup>13</sup>. The Proposal for a Regulation establishing AMLA also provides, under Article 84(1), that AMLA “may” invite “national data protection authorities” as “observers” when drafting such guidelines and recommendations.<sup>14</sup>

The EDPB considers that AMLA should closely cooperate with the EDPB when drafting guidelines or recommendations, as well as RTS. This cooperation should take place in all cases where guidelines, recommendations and RTS have “a significant impact on the protection of personal data”. In this regard, the EDPB notes that AMLA, according to Article 38 of the Proposal for Regulation establishing AMLA, shall submit the RTS to the EC for adoption by means of delegated acts pursuant to Article 290 TFEU. According to Article 42(2) of Regulation (EU) 2018/1725, the EC may consult the EDPB when preparing acts referred to in Article 42(1) (including delegated acts or implementing acts) of particular importance for the protection of individuals’ rights and freedoms with regard to the processing of personal data.

Given the potentially serious impact that RTS may have on the protection of personal data, the EDPB considers that it should be formally consulted by the EC before their adoption when they have significant impact for the protection of individuals’ rights and freedoms with regard to the processing of personal data. Furthermore, considering the impact on data protection of AMLA’s guidelines and recommendations, the EDPB calls on the legislators to assess the possibility for requiring AMLA to formally consult the EDPB before the adoption of these instruments, if they have a significant impact on the protection of personal data.

This is without prejudice to the fact that the EDPB considers that, in particular, the conditions and limits for the processing of special categories of personal data and of personal data relating to criminal

<sup>11</sup> Article 42(4) of the Proposal for a Regulation applying to the private sector.

<sup>12</sup> Article 70 GDPR

<sup>13</sup> Article 77(2) of the Proposal for a Regulation establishing AMLA.

<sup>14</sup> Article 84(1) of the Proposal for a Regulation establishing AMLA.

convictions and offences should be considered as essential elements to be defined in the legislative proposals of the AML legislative package, rather than under RTS.<sup>15</sup>

## **2. The need to better specify the conditions and limits of the processing of special categories of data and of personal data relating to criminal convictions.**

### **2.1. Regarding the processing of special categories of personal data**

Article 55(1) of the Proposal for a Regulation applying to the private sector lays down that obliged entities may process special categories of personal data referred to in Article 9(1) GDPR, to the extent that this processing is “strictly necessary for the purposes of preventing money laundering and terrorist financing”.

Article 55 does not specify the meaning of “strictly necessary”. Furthermore, the types of personal data falling under the special category of personal data that may be processed are not defined.

The EDPB points out that Article 55 might not be in line with data minimisation principle under Article 5(1)(c) GDPR and poses serious data protection concerns.<sup>16</sup> Indeed, the implementation of the provisions in Article 55 might lead obliged entities to process data falling under the scope of Article 9(1) GDPR which are not necessarily relevant for the purpose pursued, such as personal data revealing trade union membership, data concerning health, processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, and data concerning a natural person’s sex life or sexual orientation.

Therefore, the EDPB invites the co-legislators to reflect on the relevance of the processing of each special category of personal data and, following such assessment, to define explicitly under Article 55 the special categories of data that could be strictly necessary for the purpose of AML/CFT.

Furthermore, the EDPB recalls that Article 9 GDPR lays down specific rules regarding the processing of special categories of personal data according to which an exemption from the general prohibition of processing special categories of personal data is possible where the processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law. Such law allowing the processing of special categories of data 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”.<sup>17</sup>

The EDPB considers that the specific measures to safeguard the fundamental rights and interests of the data subjects provided in Article 55 are not sufficient.

---

<sup>15</sup> See EDPS opinion 12/2021, para 12.

<sup>16</sup> In the Netherlands, thousands of households were wrongly accused of fraud by the Dutch Tax authority, pushing many into serious financial problems, often triggered by ethnicity. This example shows how serious the impact of unlawful the processing of (special category of) personal data can be for EU citizens.

<sup>17</sup> See article 9(2)(g) GDPR.

Firstly, the EDPB considers that Article 55 should specify the specific purpose (preventing money laundering or terrorism financing) for which each category of personal data falling under Article 9 GDPR are likely to be processed<sup>18</sup>.

Moreover, the specific measures (identification, customer due diligence, reporting to FIU) for which these categories of personal data may be processed should also be identified by the AML legislative proposals.

In addition, for each of these categories of personal data, further specifications should be warranted in Article 55.

In order to avoid that decisions are made on a basis of discriminatory factors, it should be also specified that the assessment made by obliged entities shall not be solely based on the processing of special categories of personal data.

Furthermore, Article 55 should require the adoption by obliged entities of state-of-the-art security measures, such as access restrictions, obfuscation, encryption, pseudonymisation or disassociation.

Others safeguards could include the application of specific data minimisation techniques<sup>19</sup>, training of staff for handling special categories of personal data, as well as specific transparency and accountability provisions on the handling of special categories of personal data.

## 2.2. Regarding the processing of personal data relating to criminal convictions and offences

Article 55(3)(b) of the Proposal for a Regulation applying to the private sector lays down that obliged entities may process not only data relating to criminal convictions but also “allegations”.

The EDPB considers that the processing of such data presents a high level of risk, considering that the term “allegations” is not defined and that the sources from which information on allegations may be collected are not precisely mentioned. In addition, the EDPB notes that the impact on the person concerned could be significant (refusal for a bank to enter into a commercial relationship with the person to whom the allegation relates), whereas in some cases, the allegation could be not substantiated. Therefore, the EDPB considers that the term “allegation” should be specified in Article 55, or deleted.<sup>20</sup>

The EDPB also recalls that Article 10 GDPR lays down specific rules regarding the processing of personal data related to criminal convictions and offences. The processing of such data can be carried out when the processing is authorized by Union or Member State law providing for appropriate safeguards for the data subjects’ rights and freedoms. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

In this respect, the EDPB notes that Article 55(3)(b) provides, as specific safeguard, that obliged entities shall implement procedures that allow, when processing such data, to make the distinction

---

<sup>18</sup> Some obliged entities are currently making a distinction between the processing carried out in order to prevent and detect money laundering and those carried out in order to prevent and detect terrorist financing.

<sup>19</sup> See EDPB guidelines on Data Protection by Design and by Default, page 21, paragraph 76

<sup>20</sup> See EDPS Opinion 12/2021, para 16.

between allegations, investigations, proceedings and convictions, taking into account the fundamental right to a fair trial, the right of defense and the presumption of innocence.

Nonetheless, the EDPB considers that the safeguards for the rights and freedoms of data subjects in Article 55 are not sufficient and therefore additional safeguards should be introduced. In particular, the EDPB recommends that Article 55 specifies that allegations or judicial proceedings should not have the same impact on the risk assessment of a person as a criminal conviction.

### **3. The need to provide additional provisions in relation to the sources of information**

#### **3.1. General considerations**

According to Article 55(2)(b) of the Proposal for a Regulation applying to the private sector, obliged entities may process special categories of data covered by Article 9 GDPR “provided that the data originate from reliable sources, are accurate and up-to-date”.

The EDPB considers that the obligation to use reliable, accurate and up-to-date sources should be extended to every information processed by obliged entities for the purpose of AML/CFT.

Moreover, since the processing of inaccurate and irrelevant data would result in a breach of the principles under Articles 5(1)(c) and 5(1)(d) GDPR, to ensure compliance with these “accuracy” and “minimisation” principles, as well as with the “accountability” principle stated in article 5(2) GDPR<sup>21</sup>, the EDPB strongly recommends adding specific safeguards regarding the sources to be used by obliged entities. In particular, the EDPB suggests to include an express reference to the obligation for obliged entities to use only accurate and reliable sources (as said, for any processing of personal data), and to add a specific obligation for obliged entities to document the assessment of the reliability and accuracy of each source of information used.

#### **3.2. The need to provide specific provisions for the processing of personal data by providers of so-called “watchlists”**

A vast majority of obliged entities currently makes use of service providers (providers of so-called “watchlists”) in the context of the performance of their activities pursuant to AML/CFT requirements.

The EDPB acknowledges the need for the obliged entities to rely on this kind of services in order to fulfill their AML/CFT obligations. Providers of “watchlists” offer an easier and faster access to information to the obliged entities. Consequently, these providers could contribute to the effective implementation of the AML/CFT obligations.

However, the processing of personal data performed by these “watchlists” raises important data protection issues. The providers of these “watchlists” are acting as data controllers, as defined in Article 4(7) GDPR. They are processing special categories of personal data and personal data relating to criminal convictions and offences, the processing of which shall comply with the specific rules under Article 9 and 10 GDPR.<sup>22</sup> Moreover, the legal basis (Article 6 GDPR) for the processing of personal data

<sup>21</sup> The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')

<sup>22</sup> According to article 10 GDPR, processing of personal data relating to criminal convictions and offences shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Similarly, according to Article 9 GDPR, special categories of data can be processed only when it is necessary for reasons of substantial public interest, on the basis of Union or Member

by such providers is not clear, and the data processing at stake raise legitimate questions regarding the accuracy principle and the data minimisation principle laid down in Articles 5(1)(c) and (d) GDPR .

In light of the risks to the fundamental rights and freedoms for the data subjects and the need to provide legal certainty to these providers and to the obliged entities, the EDPB considers that specific rules might be included in the AML legislative proposals or via a dedicated EU legislative initiative.

These specific rules must be in line with GDPR requirements, and should allow, if necessary, the processing of special categories of data and of personal data relating to criminal convictions and offences under strict conditions defined in Articles 9 and 10 GDPR. The nature of personal data that can be processed by such providers according to the data minimisation principle (Article 5(1)(c) GDPR) should be specified. Strong and specific measures to safeguard the fundamental rights and the interests of the data subjects should be established too. As stated above, the EDPB considers that providing specific rules for these service providers would serve the purpose of fighting money laundering and countering terrorist financing.

In case where such rules are not provided, national supervisory authorities have the task to enforce data protection law in case of breaches by providers and obliged entities, notably regarding the processing of special categories of personal data and of personal data relating to criminal convictions and offences.

Finally, in case where specific rules would be provided for these providers, the EDPB also invites the co-legislators to include in the AML legislative proposals a reference to codes of conduct under Article 40 GDPR and to certifications under Article 42 GDPR for providers of "watchlists", to be developed taking into account the specificities of this sector.<sup>23</sup>

Yours sincerely,



Andrea Jelinek

---

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.

<sup>23</sup> See EDPS Opinion 12/2021, para 46.

# Letters



**Sent by e-mail only**

Wim Mijs, Chief Executive of the EBF  
Peter Simon, Managing Director of the ESBG  
Nina Schindler, Chief Executive Officer of the EACB  
Ralf Ohlhausen, Chair of the ETTPA  
Marcel Roy, Secretary General of the EAPB  
Elie Beyrouthy, Chair of the EPIF  
Thaer Sabri, Chief Executive Officer of the EMA  
Marc Roberts, Chair of the EFA  
Robrecht Vandormael, Secretary General of PE

Brussels, 12 May 2022

Ref: OUT2022-0031

Dear Sir/Madam,

Thank you for your letter of 31 January 2022 outlining your concerns regarding the Guidelines 06/2020 on the interplay of the Second Payment Services Directive (PSD2) and the General Data Protection Regulation (GDPR) adopted on 17 July 2020.

In response to your concerns, I would like first to highlight that the EDPB held a stakeholder event on the revised PSD2 before starting the drafting of the Guidelines. Furthermore, prior to the adoption of the final version of the Guidelines, the EDPB published a first version of the Guidelines for public consultation to collect the views and concerns of the interested stakeholders and citizens. The views that have been brought forward during these consultations -some of which mirrors the concerns raised in your letter-, have already been very carefully taken into consideration by the Board before adopting the final version of the Guidelines. As is the case with all guidance by the EDPB, the Board is permanently monitoring the necessity of reviewing these Guidelines. However, for the reasons outlined above, the EDPB considers it is not necessary to revise these Guidelines for the moment.

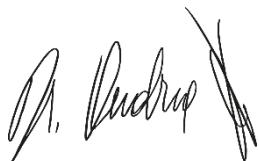
Moreover, let me recall that the EDPB has the general task of ensuring a consistent application of the GDPR (Article 70(1) GDPR), and that it is precisely to this end that it has issued these Guidelines.

In addition, supervisory authorities have the task to contribute to the consistent application of the GDPR throughout the European Union (Article 51(2) GDPR). In line with the authorities' competence to promote the awareness of controllers and processors of their obligations under the GDPR (Article

57(1) (d) GDPR), payment service providers can turn to their national supervisory authorities if they require more information and clarifications on these Guidelines.

Finally, as a suggestion, I draw your attention to the possibility for the payment sector to prepare and submit, in accordance with Article 40 of the GDPR, a code of conduct for approval by their national supervisory authority. Codes of conduct are intended to contribute to the proper application of the GDPR, taking account of the specific features of the processing sector and the specific needs of micro, small and medium-sized enterprises. The substance of this code of conduct has to be in accordance with the GDPR, also taking into account the relevant guidance provided by the EDPB. Such a code of conduct would specify the application of the GDPR in relation to the processing of personal data by payment service providers, in the context of services that fall under the PSD2, and provide further solutions and legal certainty for the sector. The EDPB Guidelines 1/2019 on codes of conduct and monitoring bodies under Regulation 2016/679<sup>1</sup> provide practical guidance and interpretative assistance.

Yours sincerely,



Andrea Jelinek

---

<sup>1</sup> [Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 | European Data Protection Board \(europa.eu\)](https://edpb.europa.eu/sites/default/files/documents/guidelines_1_2019_on_codes_of_conduct_and_monitoring_bodies_under_regulation_2016_679_en.pdf)

# Letters



Ms Mairead McGuinness  
European Commissioner for Financial services,  
financial stability and Capital Markets Union

Mr Didier Reynders  
European Commissioner for Justice

***Sent by e-mail only***

Brussels, 12 May 2022  
Ref: OUT2022-0035

Dear Commissioner McGuinness,  
Dear Commissioner Reynders,

This letter follows up on the adoption by the European Commission (“the EC”), of a legislative package of four legislative proposals (the “AML legislative proposals”) on 20 July 2021, aiming at strengthening the EU’s actions on anti-money laundering and countering the financing of terrorism (“AML/CFT”).

The legislative package includes a Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (“the Proposal for a Regulation applying to the private sector”)<sup>1</sup> and a Proposal for a Regulation of the European Parliament and of the Council establishing the European Authority for Countering Money Laundering and Financing of Terrorism (“the Proposal for a Regulation establishing AMLA”).<sup>2</sup>

The EDPB draws the attention of the European Institutions to the important data protection issues raised by the implementation of the AML/CFT obligations, as provided by the AML legislative proposals. Obligated entities are required to process personal data which allow to draw intimate

---

<sup>1</sup> COM(2021) 420 final.

<sup>2</sup> COM (2021) 421 final.

The AML legislative package also includes a Proposal for a Directive of the European Parliament and of the Council on the mechanisms for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing, and a Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets.

**Andrea Jelinek**  
Chair of the European Data Protection Board

rue Wiertz, 60  
1047 Brussels

inferences about individuals and which can notably lead to the exclusion of legal and natural persons from a right and/or a service (for instance, a banking service). It is therefore crucial that AML legislative proposals are in line with the General Data Protection Regulation (“the GDPR”).

The EDPB also underlines that ensuring a better consistency between the AML legislative proposals and GDPR principles, such as the accuracy principle or the data minimisation principle, would improve the efficiency of the implementation of the AML/CFT legal framework.

To better achieve this consistency, the EDPB calls on the EU institutions to involve the EDPB in the discussions on the AML legislative proposals and suggests some crucial modifications having regard in particular to the Proposal for a Regulation applying to the private sector and the Proposal for a Regulation establishing AMLA.

This letter partly reiterates concerns expressed by the EDPB in its Statement published in December 2020<sup>3</sup>, in a letter addressed to the EC in May 2021<sup>4</sup>, as well as in the EDPS Opinion.<sup>5</sup> Indeed, the AML legislative proposals only partially implement the recommendations issued by the EDPB in 2020 and 2021. For instance, the EDPB notes that the EC has included, as requested by the EDPB, specific provisions on the processing of special categories of data<sup>6</sup>, as well as on the processing of personal data relating to criminal convictions and offences<sup>7</sup> in the AML legislative proposals. However, the EDPB considers that the AML legislative proposals should provide for additional safeguards in relation to the processing of these personal data to ensure in particular compatibility with Articles 9 and 10 GDPR. Moreover, the AML legislative proposals do not provide specific rules in relation to the sources to be used by obliged entities for gathering information, and in relation to information provided by data service providers of so-called “watchlists”.

Without further amendments, the EDPB is of the view that the AML legislative proposals would have a disproportionate negative impact to the rights and freedoms of individuals and would lead to significant legal uncertainty. The EDPB would therefore like to highlight the following safeguards to be included in the AML legislative proposals.

## **1. Consultation of the EDPB in the context of the drafting and adoption of regulatory technical standards, guidelines and recommendations.**

The EDPB notes that regulatory technical standards (RTS), guidelines and recommendations to be developed and adopted by AMLA or the EC would, in practice, provide the core of the standardized AML/CFT rules.<sup>8</sup>

---

<sup>3</sup> EDPB Statement on the protection of personal data processed in relation with the prevention of money laundering and terrorist financing, 15 December 2020.

<sup>4</sup> EDPB letter to the European Commission on the protection of personal data in the AML-CFT legislative proposals, 19 May 2021.

<sup>5</sup> EDPS Opinion 12/2021 on the anti-money laundering and countering the financing of terrorism (AML/CFT) package of legislative proposals.

<sup>6</sup> Special categories of data are defined in Article 9 GDPR.

<sup>7</sup> Processing of personal data relating to criminal convictions and offences is regulated under Article 10 GDPR.

<sup>8</sup> The Proposal for a regulation establishing AMLA, under Article 38, lays down that AMLA develops draft regulatory technical standards (RTS) and submits them to the EC for adoption. The RTS shall be adopted by the EC by means of delegated acts pursuant to Article 290 TFEU.

Indeed, pursuant to the AML legislative proposals, the RTS shall specify, notably, the information to be collected for the purpose of performing standard, simplified and enhanced customer due diligence<sup>9</sup>. Moreover, AMLA shall issue guidelines on ongoing monitoring of a business relationship and on the monitoring of the transactions carried out in the context of such relationship<sup>10</sup>. In addition, the EC shall issue recommendations to Member States on specific rules and criteria to identify the beneficial owners of legal entities other than corporate entities.<sup>11</sup>

First of all, the EDPB considers that the categories of personal data to be processed by obliged entities and additional rules that might impact their processing should not be specified in the RTS, guidelines, and recommendations, but rather be identified directly in the AML legislative proposals.

Furthermore, in accordance with its duty to ensure a consistent application of the GDPR<sup>12</sup>, the EDPB considers that its involvement in the development of RTS, guidelines and recommendations is essential to reach a common understanding between the concerned national data protection authorities, the AMLA and the EC, to clarify the interplay of the AML CFT legal framework with the GDPR, and thus to provide legal certainty to obliged entities.

Against this background, the EDPB notes that, while Recital 58 of the Proposal for a Regulation establishing AMLA provides that the AMLA shall “closely cooperate” with the EDPB, when “developing any instruments” or “taking any decisions” having a “significant impact on the protection of personal data”, the legal text of the Proposal only includes this obligation to cooperate in relation to guidelines and recommendations, without referring to RTS<sup>13</sup>. The Proposal for a Regulation establishing AMLA also provides, under Article 84(1), that AMLA “may” invite “national data protection authorities” as “observers” when drafting such guidelines and recommendations.<sup>14</sup>

The EDPB considers that AMLA should closely cooperate with the EDPB when drafting guidelines or recommendations, as well as RTS. This cooperation should take place in all cases where guidelines, recommendations and RTS have “a significant impact on the protection of personal data”. In this regard, the EDPB notes that AMLA, according to Article 38 of the Proposal for Regulation establishing AMLA, shall submit the RTS to the EC for adoption by means of delegated acts pursuant to Article 290 TFEU. According to Article 42(2) of Regulation (EU) 2018/1725, the EC may consult the EDPB when preparing acts referred to in Article 42(1) (including delegated acts or implementing acts) of particular importance for the protection of individuals’ rights and freedoms with regard to the processing of personal data.

Given the potentially serious impact that RTS may have on the protection of personal data, the EDPB considers that it should be formally consulted by the EC before their adoption when they have significant impact for the protection of individuals’ rights and freedoms with regard to the processing of personal data. Furthermore, considering the impact on data protection of AMLA’s guidelines and recommendations, the EDPB calls on the legislators to assess the possibility for requiring AMLA to

<sup>9</sup> Article 22 of the Proposal for a Regulation applying to the private sector

<sup>10</sup> Article 21(4) of the Proposal for a Regulation applying to the private sector

<sup>11</sup> Article 42(4) of the Proposal for a Regulation applying to the private sector.

<sup>12</sup> Article 70 GDPR

<sup>13</sup> Article 77(2) of the Proposal for a Regulation establishing AMLA.

<sup>14</sup> Article 84(1) of the Proposal for a Regulation establishing AMLA.

**Andrea Jelinek**

Chair of the European Data Protection Board

rue Wiertz, 60  
1047 Brussels

formally consult the EDPB before the adoption of these instruments, if they have a significant impact on the protection of personal data.

This is without prejudice to the fact that the EDPB considers that, in particular, the conditions and limits for the processing of special categories of personal data and of personal data relating to criminal convictions and offences should be considered as essential elements to be defined in the legislative proposals of the AML legislative package, rather than under RTS.<sup>15</sup>

## 2. The need to better specify the conditions and limits of the processing of special categories of data and of personal data relating to criminal convictions.

### 2.1. Regarding the processing of special categories of personal data

Article 55(1) of the Proposal for a Regulation applying to the private sector lays down that obliged entities may process special categories of personal data referred to in Article 9(1) GDPR, to the extent that this processing is “strictly necessary for the purposes of preventing money laundering and terrorist financing”.

Article 55 does not specify the meaning of “strictly necessary”. Furthermore, the types of personal data falling under the special category of personal data that may be processed are not defined.

The EDPB points out that Article 55 might not be in line with data minimisation principle under Article 5(1)(c) GDPR and poses serious data protection concerns.<sup>16</sup> Indeed, the implementation of the provisions in Article 55 might lead obliged entities to process data falling under the scope of Article 9(1) GDPR which are not necessarily relevant for the purpose pursued, such as personal data revealing trade union membership, data concerning health, processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, and data concerning a natural person’s sex life or sexual orientation.

Therefore, the EDPB invites the co-legislators to reflect on the relevance of the processing of each special category of personal data and, following such assessment, to define explicitly under Article 55 the special categories of data that could be strictly necessary for the purpose of AML/CFT.

Furthermore, the EDPB recalls that Article 9 GDPR lays down specific rules regarding the processing of special categories of personal data according to which an exemption from the general prohibition of processing special categories of personal data is possible where the processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law. Such law allowing the processing of special categories of data 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”.<sup>17</sup>

---

<sup>15</sup> See EDPS opinion 12/2021, para 12.

<sup>16</sup> In the Netherlands, thousands of households were wrongly accused of fraud by the Dutch Tax authority, pushing many into serious financial problems, often triggered by ethnicity. This example shows how serious the impact of unlawful the processing of (special category of) personal data can be for EU citizens.

<sup>17</sup> See article 9(2)(g) GDPR.

The EDPB considers that the specific measures to safeguard the fundamental rights and interests of the data subjects provided in Article 55 are not sufficient.

Firstly, the EDPB considers that Article 55 should specify the specific purpose (preventing money laundering or terrorism financing) for which each category of personal data falling under Article 9 GDPR are likely to be processed<sup>18</sup>.

Moreover, the specific measures (identification, customer due diligence, reporting to FIU) for which these categories of personal data may be processed should also be identified by the AML legislative proposals.

In addition, for each of these categories of personal data, further specifications should be warranted in Article 55.

In order to avoid that decisions are made on a basis of discriminatory factors, it should be also specified that the assessment made by obliged entities shall not be solely based on the processing of special categories of personal data.

Furthermore, Article 55 should require the adoption by obliged entities of state-of-the-art security measures, such as access restrictions, obfuscation, encryption, pseudonymisation or disassociation.

Others safeguards could include the application of specific data minimisation techniques<sup>19</sup>, training of staff for handling special categories of personal data, as well as specific transparency and accountability provisions on the handling of special categories of personal data.

## 2.2. Regarding the processing of personal data relating to criminal convictions and offences

Article 55(3)(b) of the Proposal for a Regulation applying to the private sector lays down that obliged entities may process not only data relating to criminal convictions but also “allegations”.

The EDPB considers that the processing of such data presents a high level of risk, considering that the term “allegations” is not defined and that the sources from which information on allegations may be collected are not precisely mentioned. In addition, the EDPB notes that the impact on the person concerned could be significant (refusal for a bank to enter into a commercial relationship with the person to whom the allegation relates), whereas in some cases, the allegation could be not substantiated. Therefore, the EDPB considers that the term “allegation” should be specified in Article 55, or deleted.<sup>20</sup>

The EDPB also recalls that Article 10 GDPR lays down specific rules regarding the processing of personal data related to criminal convictions and offences. The processing of such data can be carried out when the processing is authorized by Union or Member State law providing for appropriate safeguards for the data subjects’ rights and freedoms. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

---

<sup>18</sup> Some obliged entities are currently making a distinction between the processing carried out in order to prevent and detect money laundering and those carried out in order to prevent and detect terrorist financing.

<sup>19</sup> See EDPB guidelines on Data Protection by Design and by Default, page 21, paragraph 76

<sup>20</sup> See EDPS Opinion 12/2021, para 16.

In this respect, the EDPB notes that Article 55(3)(b) provides, as specific safeguard, that obliged entities shall implement procedures that allow, when processing such data, to make the distinction between allegations, investigations, proceedings and convictions, taking into account the fundamental right to a fair trial, the right of defense and the presumption of innocence.

Nonetheless, the EDPB considers that the safeguards for the rights and freedoms of data subjects in Article 55 are not sufficient and therefore additional safeguards should be introduced. In particular, the EDPB recommends that Article 55 specifies that allegations or judicial proceedings should not have the same impact on the risk assessment of a person as a criminal conviction.

### 3. The need to provide additional provisions in relation to the sources of information

#### 3.1. General considerations

According to Article 55(2)(b) of the Proposal for a Regulation applying to the private sector, obliged entities may process special categories of data covered by Article 9 GDPR “provided that the data originate from reliable sources, are accurate and up-to-date”.

The EDPB considers that the obligation to use reliable, accurate and up-to-date sources should be extended to every information processed by obliged entities for the purpose of AML/CFT.

Moreover, since the processing of inaccurate and irrelevant data would result in a breach of the principles under Articles 5(1)(c) and 5(1)(d) GDPR, to ensure compliance with these “accuracy” and “minimisation” principles, as well as with the “accountability” principle stated in article 5(2) GDPR<sup>21</sup>, the EDPB strongly recommends adding specific safeguards regarding the sources to be used by obliged entities. In particular, the EDPB suggests to include an express reference to the obligation for obliged entities to use only accurate and reliable sources (as said, for any processing of personal data), and to add a specific obligation for obliged entities to document the assessment of the reliability and accuracy of each source of information used.

#### 3.2. The need to provide specific provisions for the processing of personal data by providers of so-called “watchlists”

A vast majority of obliged entities currently makes use of service providers (providers of so-called “watchlists”) in the context of the performance of their activities pursuant to AML/CFT requirements.

The EDPB acknowledges the need for the obliged entities to rely on this kind of services in order to fulfill their AML/CFT obligations. Providers of “watchlists” offer an easier and faster access to information to the obliged entities. Consequently, these providers could contribute to the effective implementation of the AML/CFT obligations.

However, the processing of personal data performed by these “watchlists” raises important data protection issues. The providers of these “watchlists” are acting as data controllers, as defined in Article 4(7) GDPR. They are processing special categories of personal data and personal data relating to criminal convictions and offences, the processing of which shall comply with the specific rules under

---

<sup>21</sup> The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')

Article 9 and 10 GDPR.<sup>22</sup> Moreover, the legal basis (Article 6 GDPR) for the processing of personal data by such providers is not clear, and the data processing at stake raise legitimate questions regarding the accuracy principle and the data minimisation principle laid down in Articles 5(1)(c) and (d) GDPR .

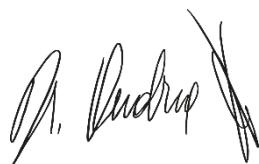
In light of the risks to the fundamental rights and freedoms for the data subjects and the need to provide legal certainty to these providers and to the obliged entities, the EDPB considers that specific rules might be included in the AML legislative proposals or via a dedicated EU legislative initiative.

These specific rules must be in line with GDPR requirements, and should allow, if necessary, the processing of special categories of data and of personal data relating to criminal convictions and offences under strict conditions defined in Articles 9 and 10 GDPR. The nature of personal data that can be processed by such providers according to the data minimisation principle (Article 5(1)(c) GDPR) should be specified. Strong and specific measures to safeguard the fundamental rights and the interests of the data subjects should be established too. As stated above, the EDPB considers that providing specific rules for these service providers would serve the purpose of fighting money laundering and countering terrorist financing.

In case where such rules are not provided, national supervisory authorities have the task to enforce data protection law in case of breaches by providers and obliged entities, notably regarding the processing of special categories of personal data and of personal data relating to criminal convictions and offences.

Finally, in case where specific rules would be provided for these providers, the EDPB also invites the co-legislators to include in the AML legislative proposals a reference to codes of conduct under Article 40 GDPR and to certifications under Article 42 GDPR for providers of “watchlists”, to be developed taking into account the specificities of this sector.<sup>23</sup>

Yours sincerely,



Andrea Jelinek

---

<sup>22</sup> According to article 10 GDPR, processing of personal data relating to criminal convictions and offences shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Similarly, according to Article 9 GDPR, special categories of data can be processed only when it is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

<sup>23</sup> See EDPS Opinion 12/2021, para 46.

# Letters



Mr Luis Garicano  
Mr Eero Heinäluoma  
ECON Committee of the European Parliament

Mr Damien Carême  
Mr Emil Radev  
LIBE Committee of the European Parliament

***Sent by e-mail only***

Brussels, 12 May 2022  
Ref: OUT2022-0036

Dear Sir,

This letter follows up on the adoption by the European Commission (“the EC”), of a legislative package of four legislative proposals (the “AML legislative proposals”) on 20 July 2021, aiming at strengthening the EU’s actions on anti-money laundering and countering the financing of terrorism (“AML/CFT”).

The legislative package includes a Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (“the Proposal for a Regulation applying to the private sector”)<sup>1</sup> and a Proposal for a Regulation of the European Parliament and of the Council establishing the European Authority for Countering Money Laundering and Financing of Terrorism (“the Proposal for a Regulation establishing AMLA”).<sup>2</sup>

The EDPB draws the attention of the European Institutions to the important data protection issues raised by the implementation of the AML/CFT obligations, as provided by the AML legislative proposals. Obligated entities are required to process personal data which allow to draw intimate inferences about individuals and which can notably lead to the exclusion of legal and natural persons

---

<sup>1</sup> COM(2021) 420 final.

<sup>2</sup> COM (2021) 421 final.

The AML legislative package also includes a Proposal for a Directive of the European Parliament and of the Council on the mechanisms for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing, and a Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets.

**Andrea Jelinek**  
Chair of the European Data Protection Board

rue Wiertz, 60  
1047 Brussels

from a right and/or a service (for instance, a banking service). It is therefore crucial that AML legislative proposals are in line with the General Data Protection Regulation (“the GDPR”).

The EDPB also underlines that ensuring a better consistency between the AML legislative proposals and GDPR principles, such as the accuracy principle or the data minimisation principle, would improve the efficiency of the implementation of the AML/CFT legal framework.

To better achieve this consistency, the EDPB calls on the EU institutions to involve the EDPB in the discussions on the AML legislative proposals and suggests some crucial modifications having regard in particular to the Proposal for a Regulation applying to the private sector and the Proposal for a Regulation establishing AMLA.

This letter partly reiterates concerns expressed by the EDPB in its Statement published in December 2020<sup>3</sup>, in a letter addressed to the EC in May 2021<sup>4</sup>, as well as in the EDPS Opinion.<sup>5</sup> Indeed, the AML legislative proposals only partially implement the recommendations issued by the EDPB in 2020 and 2021. For instance, the EDPB notes that the EC has included, as requested by the EDPB, specific provisions on the processing of special categories of data<sup>6</sup>, as well as on the processing of personal data relating to criminal convictions and offences<sup>7</sup> in the AML legislative proposals. However, the EDPB considers that the AML legislative proposals should provide for additional safeguards in relation to the processing of these personal data to ensure in particular compatibility with Articles 9 and 10 GDPR. Moreover, the AML legislative proposals do not provide specific rules in relation to the sources to be used by obliged entities for gathering information, and in relation to information provided by data service providers of so-called “watchlists”.

Without further amendments, the EDPB is of the view that the AML legislative proposals would have a disproportionate negative impact to the rights and freedoms of individuals and would lead to significant legal uncertainty. The EDPB would therefore like to highlight the following safeguards to be included in the AML legislative proposals.

### **1. Consultation of the EDPB in the context of the drafting and adoption of regulatory technical standards, guidelines and recommendations.**

The EDPB notes that regulatory technical standards (RTS), guidelines and recommendations to be developed and adopted by AMLA or the EC would, in practice, provide the core of the standardized AML/CFT rules.<sup>8</sup>

Indeed, pursuant to the AML legislative proposals, the RTS shall specify, notably, the information to be collected for the purpose of performing standard, simplified and enhanced customer due

---

<sup>3</sup> EDPB Statement on the protection of personal data processed in relation with the prevention of money laundering and terrorist financing, 15 December 2020.

<sup>4</sup> EDPB letter to the European Commission on the protection of personal data in the AML-CFT legislative proposals, 19 May 2021.

<sup>5</sup> EDPS Opinion 12/2021 on the anti-money laundering and countering the financing of terrorism (AML/CFT) package of legislative proposals.

<sup>6</sup> Special categories of data are defined in Article 9 GDPR.

<sup>7</sup> Processing of personal data relating to criminal convictions and offences is regulated under Article 10 GDPR.

<sup>8</sup> The Proposal for a regulation establishing AMLA, under Article 38, lays down that AMLA develops draft regulatory technical standards (RTS) and submits them to the EC for adoption. The RTS shall be adopted by the EC by means of delegated acts pursuant to Article 290 TFEU.

**Andrea Jelinek**  
Chair of the European Data Protection Board

rue Wiertz, 60  
1047 Brussels

diligence<sup>9</sup>. Moreover, AMLA shall issue guidelines on ongoing monitoring of a business relationship and on the monitoring of the transactions carried out in the context of such relationship<sup>10</sup>. In addition, the EC shall issue recommendations to Member States on specific rules and criteria to identify the beneficial owners of legal entities other than corporate entities.<sup>11</sup>

First of all, the EDPB considers that the categories of personal data to be processed by obliged entities and additional rules that might impact their processing should not be specified in the RTS, guidelines, and recommendations, but rather be identified directly in the AML legislative proposals.

Furthermore, in accordance with its duty to ensure a consistent application of the GDPR<sup>12</sup>, the EDPB considers that its involvement in the development of RTS, guidelines and recommendations is essential to reach a common understanding between the concerned national data protection authorities, the AMLA and the EC, to clarify the interplay of the AML CFT legal framework with the GDPR, and thus to provide legal certainty to obliged entities.

Against this background, the EDPB notes that, while Recital 58 of the Proposal for a Regulation establishing AMLA provides that the AMLA shall “closely cooperate” with the EDPB, when “developing any instruments” or “taking any decisions” having a “significant impact on the protection of personal data”, the legal text of the Proposal only includes this obligation to cooperate in relation to guidelines and recommendations, without referring to RTS<sup>13</sup>. The Proposal for a Regulation establishing AMLA also provides, under Article 84(1), that AMLA “may” invite “national data protection authorities” as “observers” when drafting such guidelines and recommendations.<sup>14</sup>

The EDPB considers that AMLA should closely cooperate with the EDPB when drafting guidelines or recommendations, as well as RTS. This cooperation should take place in all cases where guidelines, recommendations and RTS have “a significant impact on the protection of personal data”. In this regard, the EDPB notes that AMLA, according to Article 38 of the Proposal for Regulation establishing AMLA, shall submit the RTS to the EC for adoption by means of delegated acts pursuant to Article 290 TFEU. According to Article 42(2) of Regulation (EU) 2018/1725, the EC may consult the EDPB when preparing acts referred to in Article 42(1) (including delegated acts or implementing acts) of particular importance for the protection of individuals’ rights and freedoms with regard to the processing of personal data.

Given the potentially serious impact that RTS may have on the protection of personal data, the EDPB considers that it should be formally consulted by the EC before their adoption when they have significant impact for the protection of individuals’ rights and freedoms with regard to the processing of personal data. Furthermore, considering the impact on data protection of AMLA’s guidelines and recommendations, the EDPB calls on the legislators to assess the possibility for requiring AMLA to formally consult the EDPB before the adoption of these instruments, if they have a significant impact on the protection of personal data.

<sup>9</sup> Article 22 of the Proposal for a Regulation applying to the private sector

<sup>10</sup> Article 21(4) of the Proposal for a Regulation applying to the private sector

<sup>11</sup> Article 42(4) of the Proposal for a Regulation applying to the private sector.

<sup>12</sup> Article 70 GDPR

<sup>13</sup> Article 77(2) of the Proposal for a Regulation establishing AMLA.

<sup>14</sup> Article 84(1) of the Proposal for a Regulation establishing AMLA.

**Andrea Jelinek**

Chair of the European Data Protection Board

rue Wiertz, 60  
1047 Brussels

This is without prejudice to the fact that the EDPB considers that, in particular, the conditions and limits for the processing of special categories of personal data and of personal data relating to criminal convictions and offences should be considered as essential elements to be defined in the legislative proposals of the AML legislative package, rather than under RTS.<sup>15</sup>

## 2. The need to better specify the conditions and limits of the processing of special categories of data and of personal data relating to criminal convictions.

### 2.1. Regarding the processing of special categories of personal data

Article 55(1) of the Proposal for a Regulation applying to the private sector lays down that obliged entities may process special categories of personal data referred to in Article 9(1) GDPR, to the extent that this processing is “strictly necessary for the purposes of preventing money laundering and terrorist financing”.

Article 55 does not specify the meaning of “strictly necessary”. Furthermore, the types of personal data falling under the special category of personal data that may be processed are not defined.

The EDPB points out that Article 55 might not be in line with data minimisation principle under Article 5(1)(c) GDPR and poses serious data protection concerns.<sup>16</sup> Indeed, the implementation of the provisions in Article 55 might lead obliged entities to process data falling under the scope of Article 9(1) GDPR which are not necessarily relevant for the purpose pursued, such as personal data revealing trade union membership, data concerning health, processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, and data concerning a natural person’s sex life or sexual orientation.

Therefore, the EDPB invites the co-legislators to reflect on the relevance of the processing of each special category of personal data and, following such assessment, to define explicitly under Article 55 the special categories of data that could be strictly necessary for the purpose of AML/CFT.

Furthermore, the EDPB recalls that Article 9 GDPR lays down specific rules regarding the processing of special categories of personal data according to which an exemption from the general prohibition of processing special categories of personal data is possible where the processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law. Such law allowing the processing of special categories of data 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”.<sup>17</sup>

The EDPB considers that the specific measures to safeguard the fundamental rights and interests of the data subjects provided in Article 55 are not sufficient.

---

<sup>15</sup> See EDPS opinion 12/2021, para 12.

<sup>16</sup> In the Netherlands, thousands of households were wrongly accused of fraud by the Dutch Tax authority, pushing many into serious financial problems, often triggered by ethnicity. This example shows how serious the impact of unlawful the processing of (special category of) personal data can be for EU citizens.

<sup>17</sup> See article 9(2)(g) GDPR.

Firstly, the EDPB considers that Article 55 should specify the specific purpose (preventing money laundering or terrorism financing) for which each category of personal data falling under Article 9 GDPR are likely to be processed<sup>18</sup>.

Moreover, the specific measures (identification, customer due diligence, reporting to FIU) for which these categories of personal data may be processed should also be identified by the AML legislative proposals.

In addition, for each of these categories of personal data, further specifications should be warranted in Article 55.

In order to avoid that decisions are made on a basis of discriminatory factors, it should be also specified that the assessment made by obliged entities shall not be solely based on the processing of special categories of personal data.

Furthermore, Article 55 should require the adoption by obliged entities of state-of-the-art security measures, such as access restrictions, obfuscation, encryption, pseudonymisation or disassociation.

Others safeguards could include the application of specific data minimisation techniques<sup>19</sup>, training of staff for handling special categories of personal data, as well as specific transparency and accountability provisions on the handling of special categories of personal data.

## 2.2. Regarding the processing of personal data relating to criminal convictions and offences

Article 55(3)(b) of the Proposal for a Regulation applying to the private sector lays down that obliged entities may process not only data relating to criminal convictions but also “allegations”.

The EDPB considers that the processing of such data presents a high level of risk, considering that the term “allegations” is not defined and that the sources from which information on allegations may be collected are not precisely mentioned. In addition, the EDPB notes that the impact on the person concerned could be significant (refusal for a bank to enter into a commercial relationship with the person to whom the allegation relates), whereas in some cases, the allegation could be not substantiated. Therefore, the EDPB considers that the term “allegation” should be specified in Article 55, or deleted.<sup>20</sup>

The EDPB also recalls that Article 10 GDPR lays down specific rules regarding the processing of personal data related to criminal convictions and offences. The processing of such data can be carried out when the processing is authorized by Union or Member State law providing for appropriate safeguards for the data subjects’ rights and freedoms. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

In this respect, the EDPB notes that Article 55(3)(b) provides, as specific safeguard, that obliged entities shall implement procedures that allow, when processing such data, to make the distinction

---

<sup>18</sup> Some obliged entities are currently making a distinction between the processing carried out in order to prevent and detect money laundering and those carried out in order to prevent and detect terrorist financing.

<sup>19</sup> See EDPB guidelines on Data Protection by Design and by Default, page 21, paragraph 76

<sup>20</sup> See EDPS Opinion 12/2021, para 16.

between allegations, investigations, proceedings and convictions, taking into account the fundamental right to a fair trial, the right of defense and the presumption of innocence.

Nonetheless, the EDPB considers that the safeguards for the rights and freedoms of data subjects in Article 55 are not sufficient and therefore additional safeguards should be introduced. In particular, the EDPB recommends that Article 55 specifies that allegations or judicial proceedings should not have the same impact on the risk assessment of a person as a criminal conviction.

### **3. The need to provide additional provisions in relation to the sources of information**

#### **3.1. General considerations**

According to Article 55(2)(b) of the Proposal for a Regulation applying to the private sector, obliged entities may process special categories of data covered by Article 9 GDPR “provided that the data originate from reliable sources, are accurate and up-to-date”.

The EDPB considers that the obligation to use reliable, accurate and up-to-date sources should be extended to every information processed by obliged entities for the purpose of AML/CFT.

Moreover, since the processing of inaccurate and irrelevant data would result in a breach of the principles under Articles 5(1)(c) and 5(1)(d) GDPR, to ensure compliance with these “accuracy” and “minimisation” principles, as well as with the “accountability” principle stated in article 5(2) GDPR<sup>21</sup>, the EDPB strongly recommends adding specific safeguards regarding the sources to be used by obliged entities. In particular, the EDPB suggests to include an express reference to the obligation for obliged entities to use only accurate and reliable sources (as said, for any processing of personal data), and to add a specific obligation for obliged entities to document the assessment of the reliability and accuracy of each source of information used.

#### **3.2. The need to provide specific provisions for the processing of personal data by providers of so-called “watchlists”**

A vast majority of obliged entities currently makes use of service providers (providers of so-called “watchlists”) in the context of the performance of their activities pursuant to AML/CFT requirements.

The EDPB acknowledges the need for the obliged entities to rely on this kind of services in order to fulfill their AML/CFT obligations. Providers of “watchlists” offer an easier and faster access to information to the obliged entities. Consequently, these providers could contribute to the effective implementation of the AML/CFT obligations.

However, the processing of personal data performed by these “watchlists” raises important data protection issues. The providers of these “watchlists” are acting as data controllers, as defined in Article 4(7) GDPR. They are processing special categories of personal data and personal data relating to criminal convictions and offences, the processing of which shall comply with the specific rules under Article 9 and 10 GDPR.<sup>22</sup> Moreover, the legal basis (Article 6 GDPR) for the processing of personal data

---

<sup>21</sup> The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')

<sup>22</sup> According to article 10 GDPR, processing of personal data relating to criminal convictions and offences shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Similarly, according to Article 9 GDPR, special categories of data can be processed only when it is necessary for reasons of substantial public interest, on the basis of Union or Member

by such providers is not clear, and the data processing at stake raise legitimate questions regarding the accuracy principle and the data minimisation principle laid down in Articles 5(1)(c) and (d) GDPR .

In light of the risks to the fundamental rights and freedoms for the data subjects and the need to provide legal certainty to these providers and to the obliged entities, the EDPB considers that specific rules might be included in the AML legislative proposals or via a dedicated EU legislative initiative.

These specific rules must be in line with GDPR requirements, and should allow, if necessary, the processing of special categories of data and of personal data relating to criminal convictions and offences under strict conditions defined in Articles 9 and 10 GDPR. The nature of personal data that can be processed by such providers according to the data minimisation principle (Article 5(1)(c) GDPR) should be specified. Strong and specific measures to safeguard the fundamental rights and the interests of the data subjects should be established too. As stated above, the EDPB considers that providing specific rules for these service providers would serve the purpose of fighting money laundering and countering terrorist financing.

In case where such rules are not provided, national supervisory authorities have the task to enforce data protection law in case of breaches by providers and obliged entities, notably regarding the processing of special categories of personal data and of personal data relating to criminal convictions and offences.

Finally, in case where specific rules would be provided for these providers, the EDPB also invites the co-legislators to include in the AML legislative proposals a reference to codes of conduct under Article 40 GDPR and to certifications under Article 42 GDPR for providers of "watchlists", to be developed taking into account the specificities of this sector.<sup>23</sup>

Yours sincerely,



Andrea Jelinek

---

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.

<sup>23</sup> See EDPS Opinion 12/2021, para 46.

# Letters



Ursula Pachl  
BEUC, Deputy Director General

***Sent by e-mail only***

Brussels, 28 July 2022

Ref: OUT2022-0061

Dear Ms. Pachl,

With respect to your letter of 7 July 2022, please allow me to start by expressing my appreciation for the work carried out by BEUC in relation to protecting the rights of consumers in the context of the data protection legislation.

With your aforementioned letter, you drew my attention to the change of legal basis that TikTok had announced with regard to personalized advertisements. More specifically, you mentioned that TikTok informed its users that the platform would no longer seek their consent to send personalized advertisements but that as of 13 July 2022 the legal basis to send them such material would be the legitimate interest of TikTok and its partners.

In your letter you have, *inter alia*, invited the Supervisory Authorities to take swift action against this change of the privacy policy of TikTok and the EDPB to provide you with any relevant information.

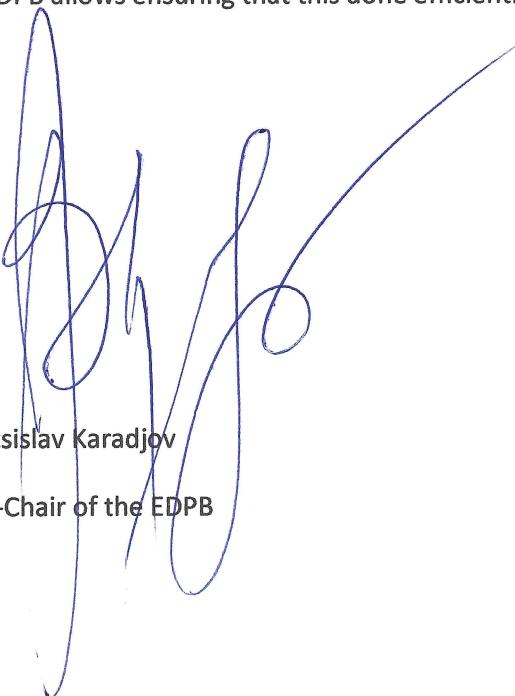
As you may already know, on 12 July 2022 TikTok announced that it would pause the change in the legal basis used for personalised ads. This outcome is the result of the immediate and efficient action that three Supervisory Authorities, namely the Irish, Italian and Spanish Supervisory Authorities, undertook in this respect from 7 until 12 July 2022.

The Italian and Spanish Supervisory Authorities took measures against TikTok on the basis of the ePrivacy Directive. On 7 July 2022, the Italian Supervisory Authority adopted a decision with a warning against TikTok on the basis of imminent violations of the ePrivacy Directive and reserved its right to take additional measures, including adopting provisional measures under Article 66(1) GDPR. On 12 July 2022, the Spanish Supervisory Authority announced that it would launch an investigation against TikTok.

On 11 July 2022, the Irish Supervisory Authority, as the lead Supervisory Authority of the platform under the GDPR engaged with TikTok with respect to the foreseen changes. Following this engagement, it was announced that the change of legal basis envisaged by TikTok would be halted.

This suspension by TikTok of the envisaged change of legal basis as the result of the swift and efficient reaction of the Supervisory Authorities highlights their determination and commitment to safeguarding the interests of the users of TikTok and of data subjects in general. Finally, I am confident that Supervisory Authorities have the necessary tools to protect the rights of data subjects and that the cooperation within the EDPB allows ensuring that this is done efficiently and consistently across the EEA countries.

Yours sincerely,



Ventsislav Karadjov

Vice-Chair of the EDPB

# Letters



Estelle Massé  
Access Now, Global Data Protection Lead,  
Isedua Oribhabor  
Access Now, Business and Human Rights Lead

*Sent by e-mail only*

Brussels, 28 July 2022

Ref: OUT2022-0062

Dear Ms. Massé, Ms. Oribhabor,

With respect to your letter of 5 July 2022, please allow me to start by expressing my appreciation for the work carried out by Access Now in relation to the protection of the rights of individuals in the context of the data protection legislation.

With your aforementioned letter, you drew my attention to the change of legal basis that TikTok had announced with regard to personalized advertisements. More specifically, you mentioned that TikTok informed its users that the platform would no longer seek their consent to send personalized advertisements but that as of 13 July 2022 the legal basis to send them such material would be the legitimate interest of TikTok and its partners.

In your letter you have, inter alia, invited the Supervisory Authorities to take swift action against this change of the privacy policy of TikTok.

As you may already know, on 12 July 2022 TikTok announced that it would pause the change in the legal basis used for personalised ads. This outcome is the result of the immediate and efficient action that three Supervisory Authorities, namely the Irish, Italian and Spanish Supervisory Authorities, undertook in this respect from 7 until 12 July 2022.

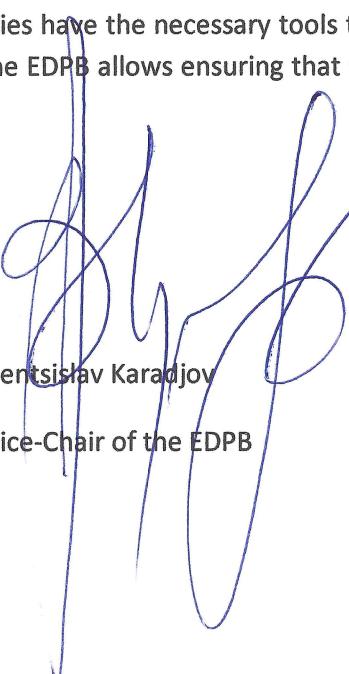
The Italian and Spanish Supervisory Authorities took measures against TikTok on the basis of the ePrivacy Directive. On 7 July 2022, the Italian Supervisory Authority adopted a decision with a warning against TikTok on the basis of imminent violations of the ePrivacy Directive and reserved its right to take additional measures, including adopting provisional measures under Article 66(1) GDPR. On 12

July 2022, the Spanish Supervisory Authority announced that it would launch an ex officio investigation against TikTok.

On 11 July 2022, the Irish Supervisory Authority, as the lead Supervisory Authority of the platform under the GDPR engaged with TikTok with respect to the foreseen changes. Following this engagement, it was announced that the change of legal basis envisaged by TikTok would be halted.

This suspension by TikTok of the envisaged change of legal basis as the result of the swift and efficient reaction of the Supervisory Authorities highlights their determination and commitment to safeguarding the interests of the users of TikTok and of data subjects in general. Finally, I am confident that Supervisory Authorities have the necessary tools to protect the rights of data subjects and that the cooperation within the EDPB allows ensuring that this is done efficiently and consistently across the EEA countries.

Yours sincerely,



Ventsislav Karadjoy

Vice-Chair of the EDPB

# Letters



Ursula Pachl  
BEUC, Deputy Director General  
***Sent by e-mail only***

Brussels, 16 September 2022

Ref: OUT2022-0064

Dear Ms. Pachl,

Thank you for your letter of 30 June 2022 with which you are bringing to my attention the complaints that BEUC and its members have submitted against Google. In your letter you are urging the EDPB to consider these complaints as a strategic case.

As you have correctly indicated, during their meeting in Vienna of last April the EDPB members committed themselves to identifying cross border cases of strategic importance where cooperation among the EDPB members would be prioritized and supported by the EDPB. As a result, on 12 July 2022 the EDPB members adopted the relevant document on the criteria and process to apply for the selection of such cases of strategic importance<sup>1</sup>.

The aforementioned adopted procedure provides that the suggestion for a case to be considered as strategic must be made by a supervisory authority and the EDPB members must agree on this.

That being said, please allow me to stress that the EDPB has already communicated your letter to its members, who will reflect on the opportunity of suggesting the complaints in question as a strategic case.

Yours sincerely,



Andrea Jelinek

---

<sup>1</sup> [https://edpb.europa.eu/our-work-tools/our-documents/other/edpb-document-selection-cases-strategic-importance\\_en](https://edpb.europa.eu/our-work-tools/our-documents/other/edpb-document-selection-cases-strategic-importance_en)

Mr Didier Reynders  
European Commissioner for Justice  
*Sent by email only*  
Brussels, 10 October 2022  
Ref.: OUT2022 -0069

Dear Commissioner Reynders,

The General Data Protection Regulation (GDPR) is a cornerstone of the digital single market and is a vital piece of legislation ensuring a human-centric approach to technology.

While its enforcement is picking up speed and the efficiency of cross-border cooperation among Supervisory Authorities is increasing steadily, the full potential of the GDPR remains to be unlocked.

With the [statement](#) adopted in April 2022, the European Data Protection Board (EDPB) signalled its enduring commitment to close cross-border cooperation. It also identified and started implementing targeted actions to enhance cooperation further, such as the identification of strategic cases for which cooperation is prioritised.

The EDPB has already developed [guidelines](#) to promote a common application of cooperation and consistency. Data Protection Authorities remain strongly committed to ensure a consistent application of the GDPR by all means at their disposal. Yet, it is a priority for GDPR cooperation to develop harmonised provisions at EU level. While recalling that it is premature to revise the GDPR at this point in time, this is necessary to iron out the differences in administrative procedures and practices which may have a detrimental impact on cross-border cooperation.

To this end, the EDPB has drawn up a list of procedural aspects that could benefit from further harmonisation at EU level, enclosed in the annex for European Commission's consideration.

This list addresses *inter alia*: the status and rights of the parties to the administrative procedures; procedural deadlines; requirements for admissibility or dismissal of complaints; investigative powers of Supervisory Authorities; and the practical implementation of the cooperation procedure.

We trust that the European Commission will support all endeavours to strengthen GDPR compliance through enforcement by addressing these procedural issues in order to maximise cross-border cooperation, and further harmonise the treatment of complainants and regulated entities across the EU.

The EDPB remains at the Commission's disposal for further information and clarifications.

Yours sincerely,



Andrea Jelinek

## Annex

As mentioned in the [EDPB Statement on enforcement cooperation](#) of 28 April 2022, Data Protection Authorities have noted that several procedural aspects could be further harmonized in EU law, in order to maximize the efficiency of the cooperation mechanism.

This annex contains a list of procedural aspects that could benefit from further harmonisation at EU level, for the consideration of the European Commission<sup>1</sup>, with a view of making sure that national procedures do not hinder the full effectiveness of the GDPR's cooperation and consistency mechanism.

### [1. Regarding the parties to the administrative procedure](#)

#### [1.1. Identification of the parties to the procedure; status and rights of the complainant](#)

##### **Proposal 1:**

- **Defining who are the parties to the procedure;**
- **Clarifying the status of the complainant as party or not;**
- **Clarifying the status and rights of representatives of complainants**

A first that could benefit from enhanced harmonisation is the extent to which the complainant is entitled to take part in the proceedings in front of the Supervisory Authority. In particular, harmonization on whether the complainant should have an active role with clearly defined rights, or whether it can only complain to the Supervisory Authority about a violation of GDPR while not being further involved in the procedure (e.g. with respect to measures and sanctions that may need to be imposed on the controller or processor)

This would entail clarifying whether the complainant is to be considered as a “party” to the procedure. In some Member States, the complainants are regarded as parties to the procedure and/or specific rights are conferred on them, while it is not the case in other Member States<sup>2</sup>.

---

<sup>1</sup> In addition to the Contribution of the EDPB to the evaluation of the GDPR under Article 97 adopted on 18 February 2020.

<sup>2</sup> The Contribution of the EDPB to the evaluation of the GDPR under Article 97 confirms, on page 11, that the complainant is “not being always perceived as a party to the proceeding before the SA”. This is also shown by the [“Overview on resources made available by Member States to the Data Protection Authorities and on enforcement actions by the Data Protection Authorities”](#) issued by the EDPB on 5 August 2021. By way of example, according to this report, complainants have a right to be heard under Austrian, Belgian, Bulgarian, Irish, Maltese, Norwegian, Polish law; on the other hand, this is not the case under Czech, French, and Swedish law. Under Spanish law, complainants are not considered as parties except where the envisaged decision may adversely affect them which is assessed on a case-by-case basis but is by default deemed to be the case in all proceedings related to the exercise of data protection rights.

Harmonisation of this aspect, regardless of the national procedural law which is used to handle the case, would avoid any different treatment of complainants depending on the Member State where the LSA is in charge or where the complaint was filed.

It would also be useful to specify that the representative mentioned in Article 80(1) GDPR, when acting on behalf of the data subject, is entitled to the same status and procedural rights as the complainant who is represented. Additionally, when this provision is implemented by Member State law, entities lodging complaints under Article 80(2) should also be treated in the same way as individual complainants.

### 1.2. Rights of the parties to the procedure

#### **Proposal 2:**

- **Specifying and harmonising procedural rights that parties are entitled to**

Procedural rights afforded to the parties<sup>3</sup> are currently different across Member States. To strengthen the uniform application of the GDPR and avoid different treatment of the parties, it would be desirable to specify a list of procedural rights that the parties are entitled to, irrespective of the Member State concerned. Increased harmonisation of the procedural rights of the parties at national level would also be beneficial in situations where the case also needs to be dealt with at EU level, in particular for cases that require dispute resolution in accordance with Article 65(1)(a) GDPR.

### 1.3. Access of the parties to the file and confidentiality

#### **Proposal 3:**

- **Specifying the right of the parties to access the documentation of the proceedings;**
- **Clarifying the minimum scope of the file;**
- **Clarifying the scope of access that should be granted to parties and further use**

In particular, the right of the parties to access the documentation of the proceedings could be further specified. In this regard, it could be useful to determine exactly what constitutes the minimum scope of the file, and the scope of the access that should be granted to the parties.

Indeed, in cooperation cases under Article 60 GDPR, there are currently no clear rules on what documents are considered part of the file, with which the parties (respondent / complainant

---

<sup>3</sup> As mentioned above, a clear identification of the parties to each procedure, with specific regard to the role of the complainant, would also be beneficial.

where relevant) have the right to acquaint themselves with, and in particular if any documents should be considered as internal and confidential documents between authorities. Without prejudice to the rights to good administration of the parties concerned, it could be clarified which documents (e.g. documents that contain formalized opinions, comments, positions and relevant and reasoned objections of Supervisory Authorities) are part of the file to which access of the parties should be granted.

Likewise, it could be beneficial to specify rules on the criteria under which documents and elements can be flagged as confidential (e.g. business secrets) by the respondent in the proceedings, and on the limitations applicable to the handling of such documents (e.g. whether they can be shared with the other parties in the proceedings).

Additionally, the specification of the rules applicable to the recipients on how they can use the information received as part of the access to the file (in terms of divulgation, for instance) would bring further clarity.

Furthermore, it should be clarified when such an access request can be addressed and which authority should process it and, if applicable, how authorities should cooperate in this process in order to have a consistent approach.

Harmonisation could also be provided on the modalities of the access to the file<sup>4</sup>.

#### 1.4. Right to be heard

**Proposal 4:**

- **Further harmonisation on scope, modalities and timing of the right to be heard of parties**

A further issue is related to the implementation of the right to be heard of the parties involved in the proceedings, before the national Supervisory Authority as it has direct consequences for the provision of this right at a later stage before the EDPB. The right to be heard is a generally recognized principle of EU law that is enshrined in Article 41 of the EU Charter of Fundamental rights. This right is currently applied in Article 60 GDPR proceedings under a patchwork of diverse Member State laws and/or practice of national supervisory authorities<sup>5</sup>.

While the need to specify which parties or subjects are entitled to this right has been outlined above, it would in addition be helpful for EU law to provide further indications as to its scope,

---

<sup>4</sup> In Poland, the parties can only get access to the documents upon an in-person appointment.

<sup>5</sup> especially relevant where national legislation is silent on this point

modalities and timing. Harmonized rules would be welcomed. For instance, when it comes to the extent and scope of this right, depending on the Member State, it may or may not be possible for a complainant to examine and react to a draft decision (and, where this possibility is provided for, this may or may not include the envisaged sanctions and corrective measures)<sup>6</sup>. Depending on the Member States, the submissions can cover only the facts and not the legal arguments. Additionally, it would be useful to harmonise the timing of the implementation of this right as the current practices currently differ<sup>7</sup>. To offer a meaningful opportunity to amend the draft decision in light of the response of the parties, the right to be heard should be implemented before the draft decision is shared with the CSAs (since the draft decision becomes final and all CSAs are bound to it unless a relevant and reasoned objection is filed). Standardizing the procedure by specifying the scope of this right, minimum standards as to modalities to be used by SAs when discharging this obligation, and the timing for documents to be shared and submissions to be taken into account, would be very useful. While the EDPB has addressed the right to be heard as part of its Rules of Procedure and in the context of specific guidelines on Article 65(1)(a), the EDPB considers that it may also be useful to codify these elements, which relate in particular to the national SAs duties and responsibilities.

## 2. Regarding procedural deadlines

### 2.1. Procedural steps not subject to a deadline

#### **Proposal 5:**

- **Further introduction of, and harmonisation of, deadlines for a number of procedural steps**
- **Further clarification of existing deadlines in the cross-border case handling procedure**
- **Introduction of rules to address the exceeding of specified or unspecified deadlines**

While GDPR specifies a number of deadlines (e.g. an SA should reply within 1 month after receiving a request in the context of article 61(2); 4 weeks to express a relevant and reasoned objection once a draft decision was submitted; 2 weeks to react on a revised draft decision, etc.), there are a number of procedural steps in the handling of a case (both at national level and in

<sup>6</sup> Please see above, footnote 2.

<sup>7</sup> The practice of the Austrian, Cypriot, Greek, Irish, Lithuanian, Luxembourgish, and Spanish SAs, as well as legislation in Latvia, Slovenia and Poland provides for hearing the parties before CSAs are consulted on the draft decision. On the other hand, the practice of the Bulgarian SA provides for CSAs to be consulted before the hearing or at least in parallel with the hearing. According to the practice of the Finnish and Portuguese SAs, the hearing should happen after sharing the draft decision. The practice of the Maltese and Dutch SAs provides for the parties to be heard at the investigation stage but not before the decision is issued.

the context of cross-border cooperation), which are not subject to any deadline. This may cause some undue delay and/or disparities in the finalization of cases<sup>8</sup>. Therefore, to foster legal certainty and avoid undermining effectiveness and credibility of enforcement, the introduction of deadlines to take a number of procedural steps could be useful (while at the same time, the time needed to process a case also depends on its complexity). This expectation is also in line with Article 41 (right to good administration) of the EU Charter of Fundamental rights and recital 129 GDPR, which highlights that the powers of supervisory authorities should be exercised within a reasonable time.

Taking into account the specificity and complexity of each case, deadlines could therefore be specified, in particular, for establishing the admissibility of the complaint, the transfer of complaints to the LSA, the establishment of the competence of the SA or LSA, to start an investigation<sup>9</sup>, to communicate the information on the case to CSAs<sup>10</sup>, to issue a draft decision<sup>11</sup>, to prepare a revised draft decision after relevant and reasoned objections were sent<sup>12</sup>, to adopt a final decision after consensus was reached, or to trigger an article 65 procedure if no consensus can be reached.

Additionally, specific provisions could be established to address situations where cross-border cases are not handled by LSA within a certain timeframe. This could be complemented by the

---

<sup>8</sup> On this, it may at the same time be relevant to bear in mind that national law or internal regulations of the SAs (SE, DK) may impose time limits for handling cases, sometimes suspended or not applicable in the case of an OSS procedure. See “[Overview on resources made available by Member States to the Data Protection Authorities and on enforcement actions by the Data Protection Authorities](#)” is issued by the EDPB on 5 August 2021 page 22.

<sup>9</sup> Including following Art. 61(2) GDPR.

<sup>10</sup> The Contribution of the EDPB to the evaluation of the GDPR under Article 97 flags, on page 10, that “the LSAs have different approaches regarding the start of the cooperation procedure, the timing of involvement of CSAs, and the communication of relevant information to them”. See the work of the EDPB on this matter within EDPB [Guidelines 02/2022 on the application of Article 60 GDPR](#).

<sup>11</sup> For instance, pursuant to Article 60.3, communicating information on the matter or submitting a draft decision must be done “without delay”. As to the timing of submission of the draft decision, the EDPB [Guidelines 02/2022 on the application of Article 60 GDPR](#) (adopted on 14 March 2022) highlight that a “timely submission of the draft decision [...] alleviates the risks for the protection of the fundamental rights and freedoms of data subjects, since corrective measures taken in due time by SAs prevent continuing infringements” (para 120), acknowledging at the same time that “bearing in mind the complexity and the variety of cases, the timeline in which the LSA needs to submit swiftly the draft decision can be quite different” (para 121). This suggests that the deadline that could be established should be a maximum deadline, without prejudice to the possibility and possibly the duty for SAs to proceed more swiftly in more straightforward cases.

<sup>12</sup> The EDPB [Guidelines 02/2022 on the application of Article 60 GDPR](#) (adopted on 14 March 2022) specify that the submission of a revised draft decision should also be carried out “without undue delay” (para 167) and that the LSA should “make sure that the lapse of time between receipt of the relevant and reasoned objections under Article 60(3) and submission of the revised draft decision is as short as possible and appropriate to the context of the OSS procedure”, “without prejudice to the efforts made to reach consensus and to the eventual obligation of the LSA to provide the right to be heard again, pursuant to national law, in view of envisaged changes in the revised draft decision that will newly affect the rights of the controller or processor” (para 168).

possibility for LSAs to provide justifications for the impossibility of meeting the deadline. This may help alleviate public criticism from complainants or the general public on some cross-border cases, which are deemed as being handled too slowly<sup>13</sup>, with no final decision being published even after a number of years.

In addition, Article 60 Section 3 of the GDPR establishes that the lead supervisory authority shall, “without delay”, communicate the relevant information on the matter to the other supervisory authorities concerned. The vagueness of the wording “without delay” poses challenges in the cooperation procedure. For legal certainty, a more precise deadline would be desirable to help enhance cooperation and the progression of cross-border cases<sup>14</sup>.

It is equally important to foresee the consequences for not complying with these newly established procedural deadlines (bearing in mind that the GDPR already provides for an ad hoc procedure which can be triggered where certain deadlines are not met<sup>15</sup>).

In addition, it would also be desirable to clarify when the administrative procedures of a supervisory authority is considered to start. In the context of cross border cases this would clarify whether the preliminary vetting by the CSA shall be counted into the administrative time limit or not, and with regard to local cases this could clarify the starting point for calculation of the deadline to take action (as some Member States have precise rules for the timeframe within which the investigation has to end).

---

<sup>13</sup> The average time for each SA to formally issue a decision on a case is analysed on page 21 of the Overview on resources made available by Member States to the Data Protection Authorities and on enforcement actions by the Data Protection Authorities” issued by the EDPB on 5 August 2021.

<sup>14</sup> The EDPB [Guidelines 02/2022 on the application of Article 60 GDPR](#) (adopted on 14 March 2022) recall that although no specific timeline is provided by Article 60, “effective enforcement of the GDPR throughout the EU requires that all CSAs receive all relevant information in a timely manner, i.e. as soon as reasonably possible” (para 54). This means that “the mutual obligation to exchange all relevant information” applies “already prior to the submission of a draft decision by the LSA” (para 54) and should be discharged “at a moment where it is still possible for the LSA to take on board the viewpoints of the other CSAs” (para 55). The EDPB then recommended “as a minimum standard” that “all efforts” should be made by the LSA to share “the scope and main conclusions of its draft decision prior to the formal submission of the latter” (para 57) with the objective of achieving consensus (see para 56).

<sup>15</sup> For instance, pursuant to Article 61.8, where a supervisory authority does not provide the information referred to in article 61.5 within one month of receiving the request of another supervisory authority, the requesting supervisory authority may adopt a provisional measure on the territory of its Member State in accordance with Article 55(1). In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an urgent binding decision from the Board pursuant to Article 66(2).

As noted above, it is important that any identified deadlines take account of the specificity and complexity of each individual case. This case by case assessment will also ensure that extensions of any specified deadline are the exception, thereby ensuring legal certainty.

### 3. Regarding complaints

#### 3.1. Formal requirements for admissibility

##### **Proposal 6:**

- **Harmonisation of formal admissibility requirements and conditions**
- **Conformation that LSAs shall not re-examine the admissibility of the complaint in cross-border cases**

The experience of the SAs shows that there is insufficient harmonization across Member States on requirements for complaints under Article 77 GDPR<sup>16</sup>. For example, in some Member States, an electronic mail suffices for the submission of a complaint, while in others, the lack of signature leads to inadmissibility of the complaint. Another example is that the name and address of the complainant may be required in some Member States, and not in others. In some countries, the complaint is inadmissible due to the lack of residency of the complainant in the State of the SA, to the fact that a prior request has not been sent to the controller, the lack of identification of legal grounds in the complaint or because the e-Gov access was not used to file the complaint. Finally, there are discrepancies as to whether the complainant has to demonstrate its interest when filing a complaint.

The “Internal EDPB Document 6/2020 on preliminary steps to handle a complaint: admissibility and vetting of complaints” states that the complaint has to fulfill formal conditions of the Member State where it was lodged, and that the LSA shall not re-examine the admissibility of the complaint<sup>17</sup>. However, this internal guidance has no binding effect on the Member State authorities.

---

<sup>16</sup> This was highlighted in the Contribution of the EDPB to the evaluation of the GDPR under Article 97, on page 10. For example, national legislation in AT, BE, BG, IT, LV, NL, PL, SI, ES foresees formal admissibility requirements. On the other hand, no admissibility requirements are foreseen in CZ, DK, DE, whereas a discretionary power regarding the assessment of admissibility is exercised in LU.

<sup>17</sup> This issue was flagged by some of the individual replies to the Questionnaire shared by the European Commission in the context of the evaluation of the GDPR: for instance, the FRSAs specified that “It appeared for instance that some DPs consider they have always to assess the admissibility of a complaint regarding their own criteria, including when they act as LSA on the basis of complaints launched with another DP. This could lead a LSA to refuse to handle a complaint, although deemed admissible by the complaint receiving DP”.

In addition, when investigating cross-border cases it is essential that the lead supervisory authority is provided with all the relevant information on the complaint, including the controller's action or lack thereof pursuant to Article 12 section 3 and 4 GDPR. Harmonized rules on the admissibility of the complaint would be desirable.

A further aspect to be considered is the harmonisation of the rules relating to the deadlines to lodge a complaint, after the data subject unsuccessfully exercised his rights<sup>18</sup>

For the consistent application of the GDPR and the equal treatment of the complainants across the EU, (i) the implementation of harmonized rules on the formal requirements of complaints, and (ii) the legal confirmation that LSAs shall not re-examine the admissibility of the complaint in cross-border cases<sup>19</sup>, could be considered.

### **3.2. Dismissal or rejection of the complaint and termination of the procedure initiated by a complaint**

#### **Proposal 7:**

- **Defining the situations that lead to rejection and dismissal of the complaint**
- **Clarifying procedural requirements for dismissal and rejection**
  - **Confirm explicitly that dismissal and rejection can be done via formal letter indicating possibility of appeal**
  - **Clarify the steps the LSA and the complaint receiving SA need to take in cases of granted appeals by either the court in country of LSA or CSA or both**

Uniform and consistent rules on the dismissal and rejection of a complaint and the termination of the procedure initiated by a complaint should be considered, as currently national rules diverge. For example, in some Member States, the lack of minimal evidence of the alleged infringement would lead to dismissal or rejection, in others the failure of response of the complainant within a reasonable timeframe results in the dismissal or rejection of the complaint or the termination of the procedure, whilst in certain Member States complaints are not filtered on their credibility or merits, nor on the necessary evidence on the alleged infringement. Defining what situations must lead to rejection or dismissal of a complaint, and what situations

---

<sup>18</sup> The proposal for the introduction of a time limitation is attributed to the recognition that the states claim is not unlimited. A time limit for introducing the complaint is envisaged in AT, SK law.

<sup>19</sup> confirming the approach agreed in the Internal EDPB Document 6/2020 available at [https://edpb.europa.eu/system/files/2022-07/internal\\_edpb\\_document\\_062020\\_on\\_admissibility\\_and\\_preliminary\\_vetting\\_of\\_complaints\\_en.pdf](https://edpb.europa.eu/system/files/2022-07/internal_edpb_document_062020_on_admissibility_and_preliminary_vetting_of_complaints_en.pdf)

may lead to the termination of the procedure is a much needed addition for the sake of consistency across the Union<sup>20</sup>.

Moreover, clarifying the procedural requirements for dismissal would be also a welcomed addendum. In particular, it would be useful to confirm explicitly that dismissal can be in form of a formal letter indicating the possibility to appeal. Finally, clarification on the need to exchange information between SAs in case of dismissal decisions regarding cross border cases would also be welcome.

Finally, it would be useful to clarify the procedure in case the complainant's appeal to the decision to dismiss or reject the complaint has been granted by the court, as in this situation, the CSA is not solely competent and the court of the CSA's Member State has no competence to force the LSA to change its decision.

### 3.3. Handling complaints with amicable settlements

#### **Proposal 8:**

- **Clear and harmonised rules on resolving complaints through amicable settlement or other non-contentious ways**
- **Clarification of the applicability of Article 60 in case of amicable settlements**

Complaints can sometimes be resolved in a non-contentious way, for example after the intervention of the SA has facilitated the exercise of the rights of a data subject<sup>21</sup>. However, the current lack of harmonisation regarding amicable settlement<sup>22</sup> creates challenges. In the majority of Member States, there is no legal framework, and therefore no possibility for the

---

<sup>20</sup> The EDPB provided, as interpretation of “dismissal or rejection”, the following: “a decision dismissing or rejecting a complaint (or parts of it) should be construed as a situation where the LSA has found, in handling the complaint, that there is no cause of action regarding the complainant's claim, and no action is taken in relation to the controller” (EDPB Guidelines 02/2022, para 225). It was also clarified by the EDPB that “a dismissal or rejection at [the cooperation stage] is different from a possible finding of dismissal or rejection at the vetting stage of the complaint procedure” since “this vetting precedes any submission of the complaint to the LSA and is performed by the complaint receiving SA” and in “such a case, the complaint would be dismissed or rejected before reaching the cooperation stage” (para 229).

<sup>21</sup> See EDPB Guidelines 02/2022 on the application of Article 60 GDPR, para 230-231; EDPB Guidelines 06/2022 on the practical implementation of amicable settlements

<sup>22</sup> This lack of harmonisation was highlighted by the Contribution of the EDPB to the evaluation of the GDPR under Article 97 on page 10-11 and 33 (“Some SAs resolve possible infringements with so-called “amicable settlements” or “amicable resolution” pursuant to provisions in their national law or explicit procedures. Other SAs aim at resolving cases in a conciliating way, even though this is not foreseen as a formal outcome of the proceedings, the case is closed when an agreement is reached between the parties or the data subject request has been satisfied. This is especially common when data subjects' rights are at stake or when minor infringements are concerned. Nine SAs did not make use of “amicable settlements”).

amicable settlements<sup>23</sup>. In addition, clear and harmonized rules on amicable settlements, including their legal status, or dedicated simplified procedures for handling such complaints are desirable.

A further issue is the need to clarify that the amicable settlement achieved in the OSS context on a specific case also requires cooperation on the legal questions behind the individual case (either by demonstrating it is an isolated case or by explaining what follow up actions are intended to be taken regarding the breach of GDPR provisions by the controller).

#### 4. Regarding investigative powers

##### **4.1. Preliminary vetting and clarification of investigatory powers of the Supervisory authorities before competence is established**

###### **Proposal 9:**

- Clarify investigatory powers of the SAs before competence pursuant to Article 55 and 56 is established (preliminary vetting)**

Experience shows that supervisory authorities have different views on the extent to which they are able to investigate processing activities and controllers to establish competence. The assessment of whether a controller or processor has a “main establishment” under Article 4(16) GDPR and thus the identification of the “lead supervisory authority” under Article 56 GDPR depends on specific requirements<sup>24</sup>. In some cases, for instance, the determination of where “decisions on the purposes and means of the processing of personal data” may require the collection of evidence. At the same time, requesting information and carrying out investigations are investigative powers as per Article 58(1) GDPR, entrusted to the competent supervisory authority. Codifying rules for preliminary vetting, steps to be followed and the clarification of the investigatory powers of the authorities before competence is established would be desirable. In particular, harmonisation could be desirable regarding the fact that complaint receiving SAs should perform preliminary investigations on the cross-border nature of complaints and, where appropriate, their potential local impact, especially for cases involving the exercise of rights.

---

<sup>23</sup> Hence, recital 131 GDPR establishing that the supervisory authority receiving a complaint or detecting or being informed otherwise of situations that entail possible infringements of the GDPR should seek an amicable settlement with the controller, cannot take real effect in many of the Member States (see Annex 2 of Guidelines 06/2022 on the practical implementation of amicable settlements).

<sup>24</sup> See the WP29 [Guidelines for identifying a controller or processor's lead supervisory authority](#), adopted on 13/12/2016, endorsed by the EDPB on 25 May 2018:

## 4.2. Investigating “to the extent appropriate”

**Proposal 10:**

- Clarifying when further investigation is and is not required

Article 57 Section 1 f) of the GDPR provides that each SA shall handle complaints lodged, and investigate, to the extent appropriate, the subject matter of the complaint. However, it is not always clear when further investigation is not required. Taking into account the independence and margins of manoeuvre of SAs to assess the elements of each case, providing indications that allow identifying cases where further investigation is not warranted would mitigate the legal uncertainty, and harmonize practices.

## 4.3. Compliance with enforcement orders

**Proposal 11:**

- Confirming that SAs are competent to monitor compliance with enforcement orders

A clear confirmation that the investigative powers of the supervisory authorities pursuant to Article 58 Section 1 GDPR include the power to monitor compliance with the enforcement orders contained in the final decision would be highly welcome. This way any remaining doubts as to the powers of SAs to monitor the adequate execution of their final decisions would be dispelled.

## 5. Regarding the cooperation procedure pursuant to Article 60 GDPR

### 5.1. Informal cooperation and scope of the information exchanged between SAs

**Proposal 13:**

- Further clarification of the scope, content and modalities of information sharing
- Clarification of the term “relevant information” in Article 60(1) and (3)
- List (types of) documents that must systematically be shared between SAs

Pursuant to Article 60 (1) and (3) GDPR, the LSA has an obligation to cooperate and share information with the CSAs also before the draft decision stage. In addition to the timing, as specified above<sup>25</sup>, the content and modalities of information sharing and cooperation during these earlier stages could be further harmonised. For instance, the current regulatory

---

<sup>25</sup> Please see footnote 12 above.

framework, which refers to a duty to share “relevant information”, is unclear about the scope and nature of the documents that must be shared with other Supervisory Authorities in the context of the OSS, both at the early stages<sup>26</sup> of the Article 60 cooperation procedure and during the different phases, in case new evidence is collected by the LSA (or CSAs). It would be useful to list unambiguously the documents that must systematically be shared between SAs<sup>27</sup>, including the initial complaint and evidence submitted by the complainant insofar relevant to the case, relevant official procedural documents adopted by the concerned supervisory authority with regard to the admissibility of the complaint, all relevant documentation pertaining to investigations carried out by the lead supervisory authority including on the scoping of the investigation, and (a summary of) the written submissions by the parties to the national proceedings. While the relevance of additional documents to be provided to other concerned supervisory authorities shall remain a matter for the lead supervisory authority to decide, draft decisions (or at least summaries of the main elements of the case and of the legal reasoning) could also be included among the relevant information that LSA share, aiming at trying to reach consensus before presenting them under the terms of article 60.3 GDPR. The LSA should also

---

<sup>26</sup> In practice, the identification of the scope of the investigation, be it in complaint-based or own volition inquiries, often causes difficulties, as to the extent to which the LSA should involve CSAs in this decision (which may rely, inter alia, on available resources, existence of parallel inquiries, enforcement strategies and other considerations) is not fully clear. The EDPB [Guidelines 09/2020 on relevant and reasoned objection](#) (V2 adopted on 09 March 2021) specify that the “system designed by the legislator suggests that consensus on the scope of the investigation should be reached at an earlier stage by the competent SAs” (para 28). More specifically: “In procedures based on a complaint or on an infringement reported by a CSA, the scope of the procedure (i.e. those aspects of data processing which are potentially the subject of a violation) should be defined by the content of the complaint or of the report shared by the CSA: in other words, it should be defined by the aspects addressed by the complaint or report. In own-volition inquiries, the LSA and CSAs should seek consensus regarding the scope of the procedure (i.e. the aspects of data processing under scrutiny) prior to initiating the procedure formally. The same applies in cases where a SA dealing with a complaint or report by another SA takes the view that an own-volition inquiry is also necessary to deal with systematic compliance issues going beyond the specific complaint or report”, para 27). However, in practice it may occur that this early involvement on the identification of the scope of the investigation does not take place. This may lead to disagreements on the scope at a time - e.g. the time when draft decisions are made available to the CSAs - where it is often too late or extremely challenging to adjust the scope of the investigation of the LSA. The EDPB has acknowledged the possibility for relevant and reasoned objections to be raised on this point, but this as a “last resort to remedy an allegedly insufficient involvement of the CSA(s) in the preceding stages of the process” (Guidelines on relevant and reasoned objections, para 28). The possible consequences of objections raised by CSAs on this point are specified in the [Guidelines on Article 65\(1\)\(a\)](#), adopted on 13 April 2021 (especially paragraphs 77-81). One way to solve this issue is by introducing provisions on a duty to agree on the scope of the investigation (it should be clarified whether this duty has different features depending on whether the case is complaint-based), e.g. via the mandatory sharing of the investigation scope in an early stage of the investigation or a mandatory meeting between the LSA and CSAs. This way, the CSAs could have greater influence on determining the scope.

<sup>27</sup> The EDPB Guidelines 02/2022 engaged in an interpretation of this wording, by specifying that the information to be considered as “relevant” “depends on the circumstances of each individual case” as it should encompass “all information that is directly or indirectly conducive to the conclusion of the proceeding” (para 46) with the goal of enabling all SAs involved to fulfil their role properly (para 47). Please see also para 48-53 for further details and specific examples of “relevant information”.

share information about the progress of the case. Confidentiality assurance related to this exchange of information would ensure that useful documents can always be shared between SAs<sup>28</sup>.

## 5.2. Information of the supervisory authorities concerned and the Board pursuant to Article 60 (7) GDPR, and moment when decisions can be published

**Proposal 14:**

- **Implement rules on the timeframe and the modalities of the obligation to inform the Board of the adoption of a decision pursuant to Article 60(7)**
- **Harmonise rules on the publication of decisions, including timeframe**

Regulating the timeframe (e.g. as soon as the decision was notified to the concerned entity vs. only after expiry of all legal remedies/appeals) and modalities (pseudonymized vs. anonymized) of the information on the adoption of the decision pursuant to Article 60 Section 7 GDPR would be desirable<sup>29</sup>.

Currently Member States have diverging rules on the moment when decisions can be published, which can lead to transparency issues and lack of a level playing field. While some Member States allow for a publication once the SA has made its decisions, others only allow publication once the decision can no longer be appealed. Related rules would be desirable in order to standardise the practices of supervisory authorities and allow for greater transparency as to the decisions adopted<sup>30</sup>.

---

<sup>28</sup> The EDPB Guidelines 02/2022 already specify that the “LSA and other CSAs may flag specific pieces of information as (highly) confidential, particularly when this seems necessary in order to meet requirements of confidentiality constraints laid down in national laws. In such a case, the SAs should inform each other immediately and jointly find legal options for a solution against the background that confidentiality provisions usually relate to external third parties and not to CSAs. In this regard, any information received that is subject to national secrecy rules should not be published or released to third parties without prior consultation with the originating authority, whenever possible” (para 52).

<sup>29</sup> See EDPB Guidelines 02/2022 (para 211-212, 215-217).

<sup>30</sup> Including via the Register of OSS Decisions kept by the EDPB.

Mr Fabien Lehagre  
President of the Association des Américains Accidentels

Mr Vincent Wellens  
NautaDutilh

Brussels, 4 November 2022

*by e-mail only*

Ref: OUT2022-0074

Dear Mr Lehagre and Mr Wellens,

Thank you for your letter of 13 April 2022 regarding the processing of personal data based on the obligations stemming from the intergovernmental agreements (IGAs) implementing the US Foreign Account Tax Compliance Act (FATCA) and your subsequent analysis on the interplay of the IGAs with the GDPR.

In your letter, you call upon the EDPB and EU supervisory authorities to take immediate action in respect of possible inconsistencies of IGAs with data protection principles set forth in the GDPR.

As already highlighted by the EDPB on other occasions, assessing the compatibility of the different IGAs implementing FATCA with the GDPR is not in the competence of the EDPB.

According to Article 70, paragraph 1 a) of the GDPR, the EDPB shall monitor and ensure the correct application of the GDPR in the cases provided for in Articles 64 and 65, without prejudice to the tasks of the EU supervisory authorities. The EDPB, as an independent European body, does not constitute a supranational institution, monitoring the work of the EU supervisory authorities in individual cases, which are subject to their territorial powers, and the EDPB has no competence to take decisions in their place.

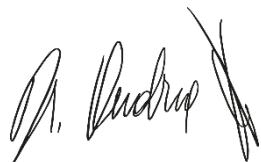
Hence, it is up to the competent supervisory authorities to monitor and enforce, where necessary, the relevant GDPR provisions and to provide information upon request on their ongoing proceedings to the extent possible according to their national procedural law.

Further, the EDPB (preceded by its precursor the Article 29 Working Party) took position on the automatic exchanges of personal data for tax purposes including FATCA, on several occasions.

More recently, in the light of the task of ensuring a consistent application of the GDPR as provided for by Article 70 GDPR and considering the existence of data protection aspects common to the different Member States, the supervisory authorities engaged in a common effort to identify questions which could be addressed to their respective competent national authorities concerning the consistency of IGAs with GDPR principles (including accountability, purpose limitation, proportionality and rules on data transfers that you specifically mentioned in your letter).

In the hope of having reassured you on the continuous attention paid by the EDPB and the supervisory authorities on the interplay between the processing based on the obligations stemming from the IGAs implementing FATCA and the GDPR, I thank you again for your consideration regarding the data protection implications of the automatic exchanges of personal data for tax purposes and the activity of the EDPB on that matter.

Yours sincerely,



Andrea Jelinek

Sophie in't Veld  
European Parliament  
Rue Wiertz 60  
B-1047 Brussels  
Belgium

Brussels, 4 November 2022

*by e-mail only*

Ref: 2022-0075

Dear Mrs in't Veld,

Let me first of all thank you for your letter of 15 June 2022 regarding the transfers of personal data based on the obligations stemming from the intergovernmental agreements (IGAs) concluded between the Member States and the US and implementing the US Foreign Account Tax Compliance Act (FATCA) and in particular, the measures taken in that respect by the supervisory authorities (SAs) and the EDPB.

With regard to the first question related to the complaints received by SAs on the above-mentioned matter, we would like to inform you that the complaint referred to in your letter and mentioned in the EDPB response of 7 July 2021 has been received by the Belgian SA. Other complaints were brought before other SAs following the publication of the statement.

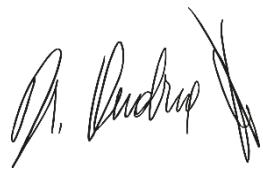
Regarding your second question about details and the state of play of the discussions of each SA with their respective government on the review of the IGA, we would like to highlight that we are not in a position to provide you with more detailed information as revealing details and the state of play of these discussions could jeopardise the actions carried out at national level.

With regards to your last question, we would like to remind you that assessing the compatibility of the different agreements concluded bilaterally between a Member State and the US with the GDPR is not within the competence of the EDPB and that it is up to the different SAs to monitor and enforce, where necessary, the protection of personal data of data subjects within their jurisdiction.

However, considering the fact that the matter concerns various Member States, the SAs decided to join in a common effort with the aim of identifying possible questions which could be addressed to their respective competent national authorities concerning the consistency of transfers based on IGAs with GDPR principles, including those of necessity and proportionality.

Please be assured that the EDPB is aware of the problematics raised by different stakeholders on this matter and it continues to offer a forum for the exchange on this topic between the different SAs.

Yours sincerely,



Andrea Jelinek



**Andrea Jelinek**  
Chair of the European Data Protection Board  
rue Wiertz, 60  
1047 Brussels

# Letters



## EDPB letter to the European Parliament, the Council, and the European Commission on data sharing for AML/CFT purposes in light of the Council's mandate for negotiations

Mr Eero Heinäluoma  
ECON Committee of the European Parliament

Mr Damien Carême  
LIBE Committee of the European Parliament

*Sent by e-mail only*

Brussels, 28 March 2023

Ref: OUT2023-0015

Dear Mr Heinäluoma,  
Dear Mr Carême,

On 20 July 2021, the European Commission has adopted a package of four legislative proposals aiming to strengthen the EU's anti-money laundering and countering the financing of terrorism<sup>1</sup>. This package includes a new Regulation on AML/CFT (hereinafter "Proposal for a Regulation on AML/CFT")<sup>2</sup> including directly-applicable rules on, inter alia, the performance of customer due diligence by obliged entities and the reporting of suspicious activity or transactions, primarily to Financial Intelligence Units (FIUs).

<sup>1</sup> European Commission, Anti-money laundering and countering the financing of terrorism legislative package, 20 July 2021, available at :[https://finance.ec.europa.eu/publications/anti-money-laundering-and-countering-financing-terrorism-legislative-package\\_en](https://finance.ec.europa.eu/publications/anti-money-laundering-and-countering-financing-terrorism-legislative-package_en). The EDPS has expressed its Opinion on this AML/CFT legislative package on 22 September 2021. The Opinion is available at: [https://edps.europa.eu/system/files/2021-09/21-09-22\\_edps-opinion-aml\\_en.pdf](https://edps.europa.eu/system/files/2021-09/21-09-22_edps-opinion-aml_en.pdf).

<sup>2</sup> European Commission, Proposal for a Regulation of the European Parliament and of the Council establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010, 20 July 2021, COM/2021/420 final, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0420>.

**Andrea Jelinek**  
Chair of the European Data Protection Board

rue Wiertz, 60  
1047 Brussels

On 5 December 2022, the Council of the European Union (Council) adopted its position on the Commission's Proposal for a Regulation on AML/CFT (hereinafter "Council's mandate")<sup>3</sup>. The Council's mandate introduces provisions that would allow, under certain conditions, obliged entities, or where applicable public authorities, that are party to the "partnership for information sharing"<sup>4</sup>, to share with each other information concerning "suspicious transactions" which is being, will be or has been reported, primarily to FIUs (**Article 54(3a)**), as well as personal data collected in the course of performing their customer due diligence obligations (**Article 55(7)**).

In addition, the Council's mandate would allow obliged entities to share between each other personal data collected in the course of performing their customer due diligence obligations, provided notably that these personal data involve "abnormalities or unusual circumstances indicating money laundering or terrorist financing" (**Article 55(5)**).

The EDPB acknowledges that the fight against money laundering and terrorism is an important public interest whose achievement deserves appropriate policies and measures. However, it reiterates the importance to strike a fair balance between this legislative objective and the interests underlying the fundamental rights to privacy and to the protection of personal data.

Any measure adopted by Member States or EU institutions in the field of AML/CFT must be compatible with Articles 7, 8 and 52(1) of the Charter of Fundamental Rights of the European Union (Charter), the GDPR, and the relevant case law. In particular, the EDPB recalls that, according to Article 52(1) of the Charter, to be lawful, any limitation to the exercise of the fundamental rights to privacy and to the protection of personal data must, *inter alia*, be provided for by law, necessary and proportionate<sup>5</sup>.

**With this letter, the EDPB draws your attention to the significant risks posed by Articles 54(3a), 55(5), 55(7) as amended by the Council's mandate to the fundamental rights to privacy and to the protection of personal data. In particular, the EDPB expresses its serious concerns as to the lawfulness, necessity, and proportionality of the above-mentioned provisions, and recommends the co-legislators not to include them in the final text of the Proposal for a Regulation on AML/CFT.**

### **1. Concerns related to the proportionality of Articles 54(3a), 55(5), and 55(7) of the Council's mandate.**

Pursuant to Article 52(1) of the Charter, legislative measures that limit the fundamental rights to privacy and to the protection of personal data should not constitute a disproportionate interference to the exercise of these rights.

---

<sup>3</sup> Council of European Union, Mandate for negotiations with the European Parliament on the Proposal for a Regulation on AML/CFT, 15517/22, 5 December 2022, available at: <https://data.consilium.europa.eu/doc/document/ST-15517-2022-INIT/en/pdf>

<sup>4</sup> In accordance with definition (42), Article 2, of the Council's proposal for amendments, "*partnership for information sharing in AML/CFT field*" refers to a "*formal cooperation established under national law between obliged entities, and where applicable, public authorities, with the purpose of supplementing compliance with this Regulation through cooperation and by sharing and processing data, in particular through the use of new technologies and artificial intelligence*".

<sup>5</sup> Pursuant to Article 52(1) of the Charter, limitation to fundamental rights may be imposed as long as it is provided for by law and respect the essence of this right. Subject to the principle of proportionality, this limitation must be necessary and genuinely meet objective of general interest recognised by the Union or the need to protect the rights and freedoms of others.

**Andrea Jelinek**  
Chair of the European Data Protection Board

rue Wiertz, 60  
1047 Brussels

The EDPB considers that the impact of Articles 54(3a), 55(5), 55(7) of the Council's mandate on the fundamental rights to privacy and to the protection of personal data would be particularly high.

The setting up of public-private partnerships ("PPPs") aiming to allow private parties (i.e. the obliged entities) to monitor subjects (i.e. their customers), on the basis of operational information provided by law enforcement authorities, and possibly related to ongoing law enforcement investigations, would entail significant risks from a data protection perspective.<sup>6</sup> In particular, the EDPB recalls that the combatting of crime is in essence a public task and that the allocation of the said task to private enterprises or PPP's should be strictly limited and thoroughly scrutinized. From a privacy and data protection perspective, limiting the flow of information from obliged entities to public authorities constitutes a safeguard for individuals. Therefore, the processing operation concerning information on possible offences arising from the reported suspicious transactions should be, in principle, limited to public authorities, given their sensitive nature and their impact on the fundamental rights of the concerned individuals.

Furthermore, the EDPB notes that the provisions proposed by the Council would allow data sharing (or data pooling) between obliged entities (without the involvement of public authorities). The data resulting from the data sharing/pooling will be used by each obliged entity to implement their AML/CFT obligations, i.e., customer due diligence obligations and reporting of suspicious transactions, if any. This implies very large scale processing, resulting in mass surveillance by private entities, the proportionality of which is highly questionable.

Lastly, the EDPB points out to the warning expressed by the Financial Action Task Force (FATF) that such data sharing may exacerbate the practice of de-risking<sup>7</sup>, which could ultimately increase the risk of undue exclusion from banking services<sup>8</sup>. Therefore, in practice, the impact of the data sharing/pooling could have serious legal consequences for the person concerned, such as difficulties in opening or accessing a current account, in using means of payment, obtaining credit, etc.

The significant risks and impacts that the Council's mandate entails, as well as the lack of studies attesting to the effectiveness of these provisions<sup>9</sup>, leads the EDPB to consider that the envisaged measures are not proportionate to the aims pursued.

---

<sup>6</sup> See EDPS, Opinion 5/2020 on the European Commission's action plan for a comprehensive Union policy on preventing money laundering and terrorism financing, 23 July 2020, paragraph 43, available at: [https://edps.europa.eu/sites/edp/files/publication/20-07-23\\_edps\\_amls\\_opinion\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/20-07-23_edps_amls_opinion_en.pdf).

<sup>7</sup> De-risking in AML/CFT is commonly defined as "*the phenomenon of financial institutions terminating or restricting business relationships with clients or categories of clients to avoid, rather than manage, risk in line with the FATF's risk-based approach.*" See at: <https://www.coe.int/en/web/moneyval/implementation/de-risking>.

<sup>8</sup> The FATF also states that "*termination of account relationships may force entities and individuals to use less regulated or unregulated channels*". FATF, Partnering in the Fight Against Financial Crime: Data protection, technology, and private sector information sharing, July 2022, paragraphs 45 and 63, available at: [https://www.fatf-gafi.org/en/publications/Digital\\_transformation/Partnering-in-the-fight-against-financial-crime.html](https://www.fatf-gafi.org/en/publications/Digital_transformation/Partnering-in-the-fight-against-financial-crime.html).

<sup>9</sup> See, in this respect, point 2 of this letter.

**Andrea Jelinek**  
Chair of the European Data Protection Board

rue Wiertz, 60  
1047 Brussels

## **2. Concerns related to the necessity of Articles 54(3a), 55(5), and 55(7) of the Council's mandate.**

Pursuant to Article 52(1) of the Charter, legislative measures that limit the fundamental rights to privacy and data protection must be necessary.

In order to ensure that the processing of personal data is carried out with due respect of the notion of necessity, one should first review the effectiveness of the proposed measures in comparison with existing or alternative less intrusive measures.

Against this background, the EDPB notes that no impact assessment was made to demonstrate the real benefit of the sharing of personal data as proposed in the Council's mandate on the fight against money laundering and terrorist financing.<sup>10</sup>

In this respect, the EDPB recalls that the necessity test implies the need for a combined, rigorous, multidisciplinary and fact-based assessment of the effectiveness of the measure for the objective pursued. Given the public interest purpose of AML/CFT, public authorities competent in AML/CFT, including at least the FIUs, should be involved in this assessment. The EDPB also recommends that the impact of data pooling on the practice of "de-risking" and the quality of suspicious transaction reports be rigorously assessed, and that this be done in conjunction with the FIUs.

Finally, the necessity test implies an assessment of whether alternative, less intrusive measures could be comparably effective for achieving the same objective.

## **3. Concerns related to the quality of legal provisions limiting the fundamental rights to privacy and to the protection of personal data.**

The EDPB recalls that, pursuant to Article 52(1) of the Charter, every limitation to the fundamental rights to privacy and to the protection of personal data must be "provided for by law". This means that limitations must be based on legal provisions that are adequately accessible and foreseeable as to their effect and formulated with sufficient precision to enable any individuals to regulate their conduct accordingly.

First, it must be examined whether the law that provides for a limitation is accessible and foreseeable. The EDPB highlights that, in presence of a law providing legal grounds for the processing of personal data, the mere existence of a law introducing (intrusive) sharing of personal data is not sufficient *per se*. Any law providing for a limitation on the fundamental rights to privacy and to the protection of personal data must fulfil specific quality requirements, namely be sufficiently detailed to ensure legal certainty and foreseeability, and provide appropriate safeguards to guarantee a fair balance between the public interest concerned, on the one hand, and the rights and freedoms of the data subjects, on the other hand. The Council's mandate, and notably Article 54(3a) thereof, while aiming at pursuing an important public interest, introduces intrusive personal data processing without adequately specifying under which conditions this processing is justified, thereby lacking the foreseeability and

---

<sup>10</sup>As the measures in the Council's mandate were not part of the initial Commission's Proposal, no such assessment was included in the Commission's impact assessment.

the legal certainty that the law should provide to all concerned natural -i.e. citizens- and legal persons, including for obliged entities that will process these personal data for AML/CFT purposes.

In addition, the EDPB considers that the provisions on data sharing in the Council's mandate do not provide adequate safeguards for data subjects. This is of special concern in the context of AML/CFT, where, as mentioned above, the provisions envisaged in the Council's mandate could result in significant impacts for individuals, such as black-listing and exclusion from financial services, in particular banking services, as well as the initiation of criminal investigations and prosecutions.

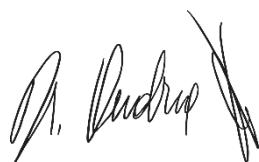
Finally, it is worth noting that the data sharing provisions in the Council's mandate might include the processing of special categories of personal data (such as personal data revealing religious belief and political opinions), the processing of which is limited to the application of strict exemptions under Article 9(2) GDPR. In this regard, it is important to note that the exemption pursuant to Article 9(2)(g) GDPR, lifting the prohibition on processing of special categories of personal data under Article 9(1) GDPR, only applies where such processing is necessary for reasons of substantial public interest on the basis of EU or Member State law is "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".

However, the EDPB considers that, given the significant risks to the fundamental rights posed by the data sharing provisions as envisaged in the Council's mandate, in particular those relating to discrimination (e.g., on the basis of religious belief or political opinion)<sup>11</sup>, as well as the lack of appropriate safeguards to mitigate them, the processing of sensitive data that would be performed in the context of these provisions cannot rely on Article 9(2)(g) GDPR.

**For all these reasons, the EDPB urges the co-legislators not to include Articles 54 (3a), 55(5), 55(7) of the Council's mandate in the final text of the AML/CFT Regulation.**

The EDPB stands ready to provide advice to the co-legislators to ensure that the policy objectives of AML/CFT are pursued in full compliance with the fundamental rights to privacy and to the protection of personal data.

Yours sincerely,



Andrea Jelinek

---

<sup>11</sup> Processing of personal data for AML purpose is likely to trigger processing of personal data on politically exposed persons, hence on political opinions.

# Letters



## EDPB letter to the European Parliament, the Council, and the European Commission on data sharing for AML/CFT purposes in light of the Council's mandate for negotiations

Ms Mairead McGuinness  
European Commissioner for Financial services,  
financial stability and Capital Markets Union

Mr Didier Reynders  
European Commissioner for Justice

***Sent by e-mail only***

Brussels, 28 March 2023  
Ref: OUT2023-0017

Dear Commissioner McGuinness,  
Dear Commissioner Reynders,

On 20 July 2021, the European Commission has adopted a package of four legislative proposals aiming to strengthen the EU's anti-money laundering and countering the financing of terrorism<sup>1</sup>. This package includes a new Regulation on AML/CFT (hereinafter "Proposal for a Regulation on AML/CFT")<sup>2</sup> including directly-applicable rules on, inter alia, the performance of customer due diligence by obliged entities and the reporting of suspicious activity or transactions, primarily to Financial Intelligence Units (FIUs).

<sup>1</sup> European Commission, Anti-money laundering and countering the financing of terrorism legislative package, 20 July 2021, available at :[https://finance.ec.europa.eu/publications/anti-money-laundering-and-countering-financing-terrorism-legislative-package\\_en](https://finance.ec.europa.eu/publications/anti-money-laundering-and-countering-financing-terrorism-legislative-package_en). The EDPS has expressed its Opinion on this AML/CFT legislative package on 22 September 2021. The Opinion is available at: [https://edps.europa.eu/system/files/2021-09/21-09-22\\_edps-opinion-aml\\_en.pdf](https://edps.europa.eu/system/files/2021-09/21-09-22_edps-opinion-aml_en.pdf)

<sup>2</sup> European Commission, Proposal for a Regulation of the European Parliament and of the Council establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010, 20 July 2021, COM/2021/420 final, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0420>

**Andrea Jelinek**  
Chair of the European Data Protection Board

rue Wiertz, 60  
1047 Brussels

On 5 December 2022, the Council of the European Union (Council) adopted its position on the Commission's Proposal for a Regulation on AML/CFT (hereinafter "Council's mandate")<sup>3</sup>. The Council's mandate introduces provisions that would allow, under certain conditions, obliged entities, or where applicable public authorities, that are party to the "partnership for information sharing"<sup>4</sup>, to share with each other information concerning "suspicious transactions" which is being, will be or has been reported, primarily to FIUs (**Article 54(3a)**), as well as personal data collected in the course of performing their customer due diligence obligations (**Article 55(7)**).

In addition, the Council's mandate would allow obliged entities to share between each other personal data collected in the course of performing their customer due diligence obligations, provided notably that these personal data involve "abnormalities or unusual circumstances indicating money laundering or terrorist financing" (**Article 55(5)**).

The EDPB acknowledges that the fight against money laundering and terrorism is an important public interest whose achievement deserves appropriate policies and measures. However, it reiterates the importance to strike a fair balance between this legislative objective and the interests underlying the fundamental rights to privacy and to the protection of personal data.

Any measure adopted by Member States or EU institutions in the field of AML/CFT must be compatible with Articles 7, 8 and 52(1) of the Charter of Fundamental Rights of the European Union (Charter), the GDPR, and the relevant case law. In particular, the EDPB recalls that, according to Article 52(1) of the Charter, to be lawful, any limitation to the exercise of the fundamental rights to privacy and to the protection of personal data must, *inter alia*, be provided for by law, necessary and proportionate<sup>5</sup>.

**With this letter, the EDPB draws your attention to the significant risks posed by Articles 54(3a), 55(5), 55(7) as amended by the Council's mandate to the fundamental rights to privacy and to the protection of personal data. In particular, the EDPB expresses its serious concerns as to the lawfulness, necessity, and proportionality of the above-mentioned provisions, and recommends the co-legislators not to include them in the final text of the Proposal for a Regulation on AML/CFT.**

### **1. Concerns related to the proportionality of Articles 54(3a), 55(5), and 55(7) of the Council's mandate.**

Pursuant to Article 52(1) of the Charter, legislative measures that limit the fundamental rights to privacy and to the protection of personal data should not constitute a disproportionate interference to the exercise of these rights.

---

<sup>3</sup> Council of European Union, Mandate for negotiations with the European Parliament on the Proposal for a Regulation on AML/CFT, 15517/22, 5 December 2022, available at: <https://data.consilium.europa.eu/doc/document/ST-15517-2022-INIT/en/pdf>

<sup>4</sup> In accordance with definition (42), Article 2, of the Council's proposal for amendments, "*partnership for information sharing in AML/CFT field*" refers to a "*formal cooperation established under national law between obliged entities, and where applicable, public authorities, with the purpose of supplementing compliance with this Regulation through cooperation and by sharing and processing data, in particular through the use of new technologies and artificial intelligence*".

<sup>5</sup> Pursuant to Article 52(1) of the Charter, limitation to fundamental rights may be imposed as long as it is provided for by law and respect the essence of this right. Subject to the principle of proportionality, this limitation must be necessary and genuinely meet objective of general interest recognised by the Union or the need to protect the rights and freedoms of others.

**Andrea Jelinek**  
Chair of the European Data Protection Board

rue Wiertz, 60  
1047 Brussels

The EDPB considers that the impact of Articles 54(3a), 55(5), 55(7) of the Council's mandate on the fundamental rights to privacy and to the protection of personal data would be particularly high.

The setting up of public-private partnerships ("PPPs") aiming to allow private parties (i.e. the obliged entities) to monitor subjects (i.e. their customers), on the basis of operational information provided by law enforcement authorities, and possibly related to ongoing law enforcement investigations, would entail significant risks from a data protection perspective.<sup>6</sup> In particular, the EDPB recalls that the combatting of crime is in essence a public task and that the allocation of the said task to private enterprises or PPP's should be strictly limited and thoroughly scrutinized. From a privacy and data protection perspective, limiting the flow of information from obliged entities to public authorities constitutes a safeguard for individuals. Therefore, the processing operation concerning information on possible offences arising from the reported suspicious transactions should be, in principle, limited to public authorities, given their sensitive nature and their impact on the fundamental rights of the concerned individuals.

Furthermore, the EDPB notes that the provisions proposed by the Council would allow data sharing (or data pooling) between obliged entities (without the involvement of public authorities). The data resulting from the data sharing/pooling will be used by each obliged entity to implement their AML/CFT obligations, i.e., customer due diligence obligations and reporting of suspicious transactions, if any. This implies very large scale processing, resulting in mass surveillance by private entities, the proportionality of which is highly questionable.

Lastly, the EDPB points out to the warning expressed by the Financial Action Task Force (FATF) that such data sharing may exacerbate the practice of de-risking<sup>7</sup>, which could ultimately increase the risk of undue exclusion from banking services<sup>8</sup>. Therefore, in practice, the impact of the data sharing/pooling could have serious legal consequences for the person concerned, such as difficulties in opening or accessing a current account, in using means of payment, obtaining credit, etc.

The significant risks and impacts that the Council's mandate entails, as well as the lack of studies attesting to the effectiveness of these provisions<sup>9</sup>, leads the EDPB to consider that the envisaged measures are not proportionate to the aims pursued.

---

<sup>6</sup> See EDPS, Opinion 5/2020 on the European Commission's action plan for a comprehensive Union policy on preventing money laundering and terrorism financing, 23 July 2020, paragraph 43, available at: [https://edps.europa.eu/sites/edp/files/publication/20-07-23\\_edps\\_amls\\_opinion\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/20-07-23_edps_amls_opinion_en.pdf).

<sup>7</sup> De-risking in AML/CFT is commonly defined as "*the phenomenon of financial institutions terminating or restricting business relationships with clients or categories of clients to avoid, rather than manage, risk in line with the FATF's risk-based approach.*" See at: <https://www.coe.int/en/web/moneyval/implementation/de-risking>.

<sup>8</sup> The FATF also states that "*termination of account relationships may force entities and individuals to use less regulated or unregulated channels*". FATF, Partnering in the Fight Against Financial Crime: Data protection, technology, and private sector information sharing, July 2022, paragraphs 45 and 63, available at: [https://www.fatf-gafi.org/en/publications/Digital\\_transformation/Partnering-in-the-fight-against-financial-crime.html](https://www.fatf-gafi.org/en/publications/Digital_transformation/Partnering-in-the-fight-against-financial-crime.html).

<sup>9</sup> See, in this respect, point 2 of this letter.

**Andrea Jelinek**  
Chair of the European Data Protection Board

rue Wiertz, 60  
1047 Brussels

## **2. Concerns related to the necessity of Articles 54(3a), 55(5), and 55(7) of the Council's mandate.**

Pursuant to Article 52(1) of the Charter, legislative measures that limit the fundamental rights to privacy and data protection must be necessary.

In order to ensure that the processing of personal data is carried out with due respect of the notion of necessity, one should first review the effectiveness of the proposed measures in comparison with existing or alternative less intrusive measures.

Against this background, the EDPB notes that no impact assessment was made to demonstrate the real benefit of the sharing of personal data as proposed in the Council's mandate on the fight against money laundering and terrorist financing.<sup>10</sup>

In this respect, the EDPB recalls that the necessity test implies the need for a combined, rigorous, multidisciplinary and fact-based assessment of the effectiveness of the measure for the objective pursued. Given the public interest purpose of AML/CFT, public authorities competent in AML/CFT, including at least the FIUs, should be involved in this assessment. The EDPB also recommends that the impact of data pooling on the practice of "de-risking" and the quality of suspicious transaction reports be rigorously assessed, and that this be done in conjunction with the FIUs.

Finally, the necessity test implies an assessment of whether alternative, less intrusive measures could be comparably effective for achieving the same objective.

## **3. Concerns related to the quality of legal provisions limiting the fundamental rights to privacy and to the protection of personal data.**

The EDPB recalls that, pursuant to Article 52(1) of the Charter, every limitation to the fundamental rights to privacy and to the protection of personal data must be "provided for by law". This means that limitations must be based on legal provisions that are adequately accessible and foreseeable as to their effect and formulated with sufficient precision to enable any individuals to regulate their conduct accordingly.

First, it must be examined whether the law that provides for a limitation is accessible and foreseeable. The EDPB highlights that, in presence of a law providing legal grounds for the processing of personal data, the mere existence of a law introducing (intrusive) sharing of personal data is not sufficient *per se*. Any law providing for a limitation on the fundamental rights to privacy and to the protection of personal data must fulfil specific quality requirements, namely be sufficiently detailed to ensure legal certainty and foreseeability, and provide appropriate safeguards to guarantee a fair balance between the public interest concerned, on the one hand, and the rights and freedoms of the data subjects, on the other hand. The Council's mandate, and notably Article 54(3a) thereof, while aiming at pursuing an important public interest, introduces intrusive personal data processing without adequately specifying under which conditions this processing is justified, thereby lacking the foreseeability and

---

<sup>10</sup>As the measures in the Council's mandate were not part of the initial Commission's Proposal, no such assessment was included in the Commission's impact assessment.

the legal certainty that the law should provide to all concerned natural -i.e. citizens- and legal persons, including for obliged entities that will process these personal data for AML/CFT purposes.

In addition, the EDPB considers that the provisions on data sharing in the Council's mandate do not provide adequate safeguards for data subjects. This is of special concern in the context of AML/CFT, where, as mentioned above, the provisions envisaged in the Council's mandate could result in significant impacts for individuals, such as black-listing and exclusion from financial services, in particular banking services, as well as the initiation of criminal investigations and prosecutions.

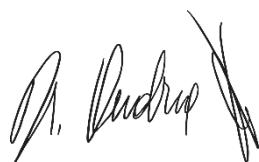
Finally, it is worth noting that the data sharing provisions in the Council's mandate might include the processing of special categories of personal data (such as personal data revealing religious belief and political opinions), the processing of which is limited to the application of strict exemptions under Article 9(2) GDPR. In this regard, it is important to note that the exemption pursuant to Article 9(2)(g) GDPR, lifting the prohibition on processing of special categories of personal data under Article 9(1) GDPR, only applies where such processing is necessary for reasons of substantial public interest on the basis of EU or Member State law is "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".

However, the EDPB considers that, given the significant risks to the fundamental rights posed by the data sharing provisions as envisaged in the Council's mandate, in particular those relating to discrimination (e.g., on the basis of religious belief or political opinion)<sup>11</sup>, as well as the lack of appropriate safeguards to mitigate them, the processing of sensitive data that would be performed in the context of these provisions cannot rely on Article 9(2)(g) GDPR.

**For all these reasons, the EDPB urges the co-legislators not to include Articles 54 (3a), 55(5), 55(7) of the Council's mandate in the final text of the AML/CFT Regulation.**

The EDPB stands ready to provide advice to the co-legislators to ensure that the policy objectives of AML/CFT are pursued in full compliance with the fundamental rights to privacy and to the protection of personal data.

Yours sincerely,



Andrea Jelinek

---

<sup>11</sup> Processing of personal data for AML purpose is likely to trigger processing of personal data on politically exposed persons, hence on political opinions.

# Letters



## EDPB letter to the European Parliament, the Council, and the European Commission on data sharing for AML/CFT purposes in light of the Council's mandate for negotiations

Ms Elisabeth Svantesson

Minister of Finance

Mr Lars Danielsson

Permanent Representative to the EU

***Sent by e-mail only***

Brussels, 28 March 2023

Ref: OUT2023-0018

Dear Ms Svantesson,

Dear Mr Danielsson,

On 20 July 2021, the European Commission has adopted a package of four legislative proposals aiming to strengthen the EU's anti-money laundering and countering the financing of terrorism<sup>1</sup>. This package includes a new Regulation on AML/CFT (hereinafter "Proposal for a Regulation on AML/CFT")<sup>2</sup> including directly-applicable rules on, inter alia, the performance of customer due diligence by obliged entities and the reporting of suspicious activity or transactions, primarily to Financial Intelligence Units (FIUs).

<sup>1</sup> European Commission, Anti-money laundering and countering the financing of terrorism legislative package, 20 July 2021, available at :[https://finance.ec.europa.eu/publications/anti-money-laundering-and-countering-financing-terrorism-legislative-package\\_en](https://finance.ec.europa.eu/publications/anti-money-laundering-and-countering-financing-terrorism-legislative-package_en). The EDPS has expressed its Opinion on this AML/CFT legislative package on 22 September 2021. The Opinion is available at: [https://edps.europa.eu/system/files/2021-09/21-09-22\\_edps-opinion-aml\\_en.pdf](https://edps.europa.eu/system/files/2021-09/21-09-22_edps-opinion-aml_en.pdf).

<sup>2</sup> European Commission, Proposal for a Regulation of the European Parliament and of the Council establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010, 20 July 2021, COM/2021/420 final, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0420>.

**Andrea Jelinek**

Chair of the European Data Protection Board

rue Wiertz, 60  
1047 Brussels

On 5 December 2022, the Council of the European Union (Council) adopted its position on the Commission's Proposal for a Regulation on AML/CFT (hereinafter "Council's mandate")<sup>3</sup>. The Council's mandate introduces provisions that would allow, under certain conditions, obliged entities, or where applicable public authorities, that are party to the "partnership for information sharing"<sup>4</sup>, to share with each other information concerning "suspicious transactions" which is being, will be or has been reported, primarily to FIUs (**Article 54(3a)**), as well as personal data collected in the course of performing their customer due diligence obligations (**Article 55(7)**).

In addition, the Council's mandate would allow obliged entities to share between each other personal data collected in the course of performing their customer due diligence obligations, provided notably that these personal data involve "abnormalities or unusual circumstances indicating money laundering or terrorist financing" (**Article 55(5)**).

The EDPB acknowledges that the fight against money laundering and terrorism is an important public interest whose achievement deserves appropriate policies and measures. However, it reiterates the importance to strike a fair balance between this legislative objective and the interests underlying the fundamental rights to privacy and to the protection of personal data.

Any measure adopted by Member States or EU institutions in the field of AML/CFT must be compatible with Articles 7, 8 and 52(1) of the Charter of Fundamental Rights of the European Union (Charter), the GDPR, and the relevant case law. In particular, the EDPB recalls that, according to Article 52(1) of the Charter, to be lawful, any limitation to the exercise of the fundamental rights to privacy and to the protection of personal data must, *inter alia*, be provided for by law, necessary and proportionate<sup>5</sup>.

**With this letter, the EDPB draws your attention to the significant risks posed by Articles 54(3a), 55(5), 55(7) as amended by the Council's mandate to the fundamental rights to privacy and to the protection of personal data. In particular, the EDPB expresses its serious concerns as to the lawfulness, necessity, and proportionality of the above-mentioned provisions, and recommends the co-legislators not to include them in the final text of the Proposal for a Regulation on AML/CFT.**

### **1. Concerns related to the proportionality of Articles 54(3a), 55(5), and 55(7) of the Council's mandate.**

Pursuant to Article 52(1) of the Charter, legislative measures that limit the fundamental rights to privacy and to the protection of personal data should not constitute a disproportionate interference to the exercise of these rights.

---

<sup>3</sup> Council of European Union, Mandate for negotiations with the European Parliament on the Proposal for a Regulation on AML/CFT, 15517/22, 5 December 2022, available at: <https://data.consilium.europa.eu/doc/document/ST-15517-2022-INIT/en/pdf>

<sup>4</sup> In accordance with definition (42), Article 2, of the Council's proposal for amendments, "*partnership for information sharing in AML/CFT field*" refers to a "*formal cooperation established under national law between obliged entities, and where applicable, public authorities, with the purpose of supplementing compliance with this Regulation through cooperation and by sharing and processing data, in particular through the use of new technologies and artificial intelligence*".

<sup>5</sup> Pursuant to Article 52(1) of the Charter, limitation to fundamental rights may be imposed as long as it is provided for by law and respect the essence of this right. Subject to the principle of proportionality, this limitation must be necessary and genuinely meet objective of general interest recognised by the Union or the need to protect the rights and freedoms of others.

**Andrea Jelinek**  
Chair of the European Data Protection Board

rue Wiertz, 60  
1047 Brussels

The EDPB considers that the impact of Articles 54(3a), 55(5), 55(7) of the Council's mandate on the fundamental rights to privacy and to the protection of personal data would be particularly high.

The setting up of public-private partnerships ("PPPs") aiming to allow private parties (i.e. the obliged entities) to monitor subjects (i.e. their customers), on the basis of operational information provided by law enforcement authorities, and possibly related to ongoing law enforcement investigations, would entail significant risks from a data protection perspective.<sup>6</sup> In particular, the EDPB recalls that the combatting of crime is in essence a public task and that the allocation of the said task to private enterprises or PPP's should be strictly limited and thoroughly scrutinized. From a privacy and data protection perspective, limiting the flow of information from obliged entities to public authorities constitutes a safeguard for individuals. Therefore, the processing operation concerning information on possible offences arising from the reported suspicious transactions should be, in principle, limited to public authorities, given their sensitive nature and their impact on the fundamental rights of the concerned individuals.

Furthermore, the EDPB notes that the provisions proposed by the Council would allow data sharing (or data pooling) between obliged entities (without the involvement of public authorities). The data resulting from the data sharing/pooling will be used by each obliged entity to implement their AML/CFT obligations, i.e., customer due diligence obligations and reporting of suspicious transactions, if any. This implies very large scale processing, resulting in mass surveillance by private entities, the proportionality of which is highly questionable.

Lastly, the EDPB points out to the warning expressed by the Financial Action Task Force (FATF) that such data sharing may exacerbate the practice of de-risking<sup>7</sup>, which could ultimately increase the risk of undue exclusion from banking services<sup>8</sup>. Therefore, in practice, the impact of the data sharing/pooling could have serious legal consequences for the person concerned, such as difficulties in opening or accessing a current account, in using means of payment, obtaining credit, etc.

The significant risks and impacts that the Council's mandate entails, as well as the lack of studies attesting to the effectiveness of these provisions<sup>9</sup>, leads the EDPB to consider that the envisaged measures are not proportionate to the aims pursued.

---

<sup>6</sup> See EDPS, Opinion 5/2020 on the European Commission's action plan for a comprehensive Union policy on preventing money laundering and terrorism financing, 23 July 2020, paragraph 43, available at: [https://edps.europa.eu/sites/edp/files/publication/20-07-23\\_edps\\_amls\\_opinion\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/20-07-23_edps_amls_opinion_en.pdf).

<sup>7</sup> De-risking in AML/CFT is commonly defined as "*the phenomenon of financial institutions terminating or restricting business relationships with clients or categories of clients to avoid, rather than manage, risk in line with the FATF's risk-based approach.*" See at: <https://www.coe.int/en/web/moneyval/implementation/de-risking>.

<sup>8</sup> The FATF also states that "*termination of account relationships may force entities and individuals to use less regulated or unregulated channels*". FATF, Partnering in the Fight Against Financial Crime: Data protection, technology, and private sector information sharing, July 2022, paragraphs 45 and 63, available at: [https://www.fatf-gafi.org/en/publications/Digital\\_transformation/Partnering-in-the-fight-against-financial-crime.html](https://www.fatf-gafi.org/en/publications/Digital_transformation/Partnering-in-the-fight-against-financial-crime.html).

<sup>9</sup> See, in this respect, point 2 of this letter.

**Andrea Jelinek**  
Chair of the European Data Protection Board

rue Wiertz, 60  
1047 Brussels

## **2. Concerns related to the necessity of Articles 54(3a), 55(5), and 55(7) of the Council's mandate.**

Pursuant to Article 52(1) of the Charter, legislative measures that limit the fundamental rights to privacy and data protection must be necessary.

In order to ensure that the processing of personal data is carried out with due respect of the notion of necessity, one should first review the effectiveness of the proposed measures in comparison with existing or alternative less intrusive measures.

Against this background, the EDPB notes that no impact assessment was made to demonstrate the real benefit of the sharing of personal data as proposed in the Council's mandate on the fight against money laundering and terrorist financing.<sup>10</sup>

In this respect, the EDPB recalls that the necessity test implies the need for a combined, rigorous, multidisciplinary and fact-based assessment of the effectiveness of the measure for the objective pursued. Given the public interest purpose of AML/CFT, public authorities competent in AML/CFT, including at least the FIUs, should be involved in this assessment. The EDPB also recommends that the impact of data pooling on the practice of "de-risking" and the quality of suspicious transaction reports be rigorously assessed, and that this be done in conjunction with the FIUs.

Finally, the necessity test implies an assessment of whether alternative, less intrusive measures could be comparably effective for achieving the same objective.

## **3. Concerns related to the quality of legal provisions limiting the fundamental rights to privacy and to the protection of personal data.**

The EDPB recalls that, pursuant to Article 52(1) of the Charter, every limitation to the fundamental rights to privacy and to the protection of personal data must be "provided for by law". This means that limitations must be based on legal provisions that are adequately accessible and foreseeable as to their effect and formulated with sufficient precision to enable any individuals to regulate their conduct accordingly.

First, it must be examined whether the law that provides for a limitation is accessible and foreseeable. The EDPB highlights that, in presence of a law providing legal grounds for the processing of personal data, the mere existence of a law introducing (intrusive) sharing of personal data is not sufficient *per se*. Any law providing for a limitation on the fundamental rights to privacy and to the protection of personal data must fulfil specific quality requirements, namely be sufficiently detailed to ensure legal certainty and foreseeability, and provide appropriate safeguards to guarantee a fair balance between the public interest concerned, on the one hand, and the rights and freedoms of the data subjects, on the other hand. The Council's mandate, and notably Article 54(3a) thereof, while aiming at pursuing an important public interest, introduces intrusive personal data processing without adequately specifying under which conditions this processing is justified, thereby lacking the foreseeability and

---

<sup>10</sup>As the measures in the Council's mandate were not part of the initial Commission's Proposal, no such assessment was included in the Commission's impact assessment.

the legal certainty that the law should provide to all concerned natural -i.e. citizens- and legal persons, including for obliged entities that will process these personal data for AML/CFT purposes.

In addition, the EDPB considers that the provisions on data sharing in the Council's mandate do not provide adequate safeguards for data subjects. This is of special concern in the context of AML/CFT, where, as mentioned above, the provisions envisaged in the Council's mandate could result in significant impacts for individuals, such as black-listing and exclusion from financial services, in particular banking services, as well as the initiation of criminal investigations and prosecutions.

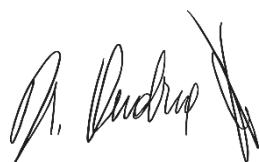
Finally, it is worth noting that the data sharing provisions in the Council's mandate might include the processing of special categories of personal data (such as personal data revealing religious belief and political opinions), the processing of which is limited to the application of strict exemptions under Article 9(2) GDPR. In this regard, it is important to note that the exemption pursuant to Article 9(2)(g) GDPR, lifting the prohibition on processing of special categories of personal data under Article 9(1) GDPR, only applies where such processing is necessary for reasons of substantial public interest on the basis of EU or Member State law is "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".

However, the EDPB considers that, given the significant risks to the fundamental rights posed by the data sharing provisions as envisaged in the Council's mandate, in particular those relating to discrimination (e.g., on the basis of religious belief or political opinion)<sup>11</sup>, as well as the lack of appropriate safeguards to mitigate them, the processing of sensitive data that would be performed in the context of these provisions cannot rely on Article 9(2)(g) GDPR.

**For all these reasons, the EDPB urges the co-legislators not to include Articles 54 (3a), 55(5), 55(7) of the Council's mandate in the final text of the AML/CFT Regulation.**

The EDPB stands ready to provide advice to the co-legislators to ensure that the policy objectives of AML/CFT are pursued in full compliance with the fundamental rights to privacy and to the protection of personal data.

Yours sincerely,



Andrea Jelinek

---

<sup>11</sup> Processing of personal data for AML purpose is likely to trigger processing of personal data on politically exposed persons, hence on political opinions.

**Anu Talus**

Chair of the European Data Protection Board

Emily O'Reilly  
European Ombudsman  
1 avenue du President Robert Schuman  
F-67001 Strasbourg Cedex  
France

Brussels, 28 June 2023

*by e-mail only*

Ref: OUT2023-0046

**EDPB Response to the European Ombudsman's recommendation regarding joined cases 509/2022/JK and 1698/2022/JK**

Dear Ms O'Reilly,

The EDPB is grateful for your letter of 29 March 2023 enclosing your recommendation on joined cases 509/2022/JK and 1698/2022/JK (the “**Recommendation**”), including the confidential annex providing a more detailed assessment on the nature and content of the preparatory documents. The EDPB thanks you for your Recommendation.

As we have noted in our previous correspondence, the EDPB values transparency and is committed to open decision-making and good administration. The EDPB takes a finding of maladministration very seriously and has used this opportunity to review this complaint. Your Recommendation was discussed during the Plenary meetings of the 24-25 May and 20 June 2023.

The EDPB fully supports providing the broadest possible access to the documents at issue, in compliance with Regulation (EC) No 1049/2001 and agrees with your Recommendation. The Court of Justice of the European Union (CJEU) has yet to deliberate and confirm in case law some of the matters in scope of this complaint. In the meantime and in the spirit of transparency and cooperation, the EDPB has endeavoured to achieve your proposed balanced solution. The EDPB agrees to disclose draft European Data Protection Board  
Rue Wiertz, 60  
1047 Brussels

versions of documents in scope of the complaint, including with tracked changes, and agrees with your proposal to anonymise such documents so that they are unable to attribute views to a specific author.

The EDPB is pleased to provide you with our opinion in response to your Recommendation. In this opinion, the EDPB has presented the decision taken by the Plenary regarding the different categories of documents, before providing a detailed response to your assessment. We of course remain at your disposal should you wish to engage on these matters bilaterally.

## **1. The EDPB's position regarding the disclosure for each category of documents, following the Ombudsman's Recommendation**

Following a reassessment of all the documents in scope of your Recommendation, the EDPB members have discussed this matter during its recent Plenaries of 24 May and 20 June 2023. Consequently, the EDPB has decided to revise its confirmatory decision regarding the disclosure of these documents, in order to grant the widest possible access to them, and fully comply with your Recommendation. The revised EDPB position is set out below, for each category of documents subject to your Recommendation.

### **2.1. Draft versions of EDPB Statement 04/2021<sup>1</sup>**

#### **Case 509/2022**

In its confirmatory decision, the EDPB has denied access to 8 draft versions<sup>2</sup> subject to your Recommendation. After a re-assessment of these documents and taking into consideration your Recommendation, the EDPB has decided to:

- **Fully disclose 7 of these drafts<sup>3</sup>.**
- **Partially disclose the remaining draft<sup>4</sup>. This document will be disclosed in an anonymised form.** The internal comments will not be disclosed, because the EDPB considers that redacting the reference to the supervisory authorities ("SAs") which made the comments is not sufficient to ensure the document is anonymised. The EDPB has therefore decided that the contents of these internal comments shall remain confidential, and that the exception of Article 4(3) 2<sup>nd</sup> paragraph of Regulation (EC) No 1049/2001 is applicable in this case. The EDPB is committed to ensuring transparency of its decision-making process, and considers that this is achieved by granting access to the track changes in the document. The EDPB has provided its detailed reasoning on this matter below under Section 2.

---

<sup>1</sup> EDPB Statement 04/2021 on international agreements including transfers, adopted on 13 April 2021. Available at [https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-042021-international-agreements-including\\_en](https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-042021-international-agreements-including_en).

<sup>2</sup> Documents 19, 20, 21, 22, 23, 24, 25, 26.

<sup>3</sup> Documents 19, 20, 21, 22, 24, 25, 26.

<sup>4</sup> Document 23.

## Case 1698/2022

In its confirmatory decision, the EDPB has denied access to 7 draft versions<sup>5</sup> subject to your Recommendation. After a re-assessment of these documents, and taking into consideration your Recommendation, the EDPB has decided to **fully disclose all 7 of these drafts**.

The remaining two categories of documents only concern case 509/2022.

### 2.1. Minutes and draft minutes of expert subgroup meetings

In its confirmatory decision, the EDPB has denied access to 4 draft versions<sup>6</sup> subject to your Recommendation. After a re-assessment, and taking into consideration your Recommendation, the EDPB has decided to fully disclose the draft minutes to the extent that they fall within the scope of the request. Therefore, the EDPB will provide the draft minutes to the applicant fully disclosing section 7 thereof.

### 2.1. E-mail exchanges between the European Commission and the EDPB, as well as EDPB members and the EDPB Secretariat

In its initial decision, the EDPB has granted partial access to 3 documents which contain e-mails<sup>7</sup> subject to your Recommendation. After a re-assessment of these documents, and taking into consideration your Recommendation, the EDPB has decided to confirm its position with respect to the parts which were not disclosed, and maintains that the exception of Article 4(3)2<sup>nd</sup> paragraph of Regulation (EC) No 1049/2001 is applicable in this case<sup>8</sup>, and that it has granted the broadest possible access without undermining the decision-making process of the EDPB. As regards document 8, the EDPB maintains its position with regard to one sentence, concerning a matter on which the EDPB has not yet decided, and considers that the exception of Article 4(3)1st paragraph of Regulation (EC) No 1049/2001 is applicable in this case. The EDPB has provided its detailed reasoning on this matter below under Section 2.

The EDPB notes that your Recommendation seems to identify issues with two e-mails, hence the EDPB would like to take the opportunity to provide some clarifications in this respect.

---

<sup>5</sup> Documents 1, 2, 3, 4, 5, 6, 7.

<sup>6</sup> Documents 1, 2, 3, 4. Please note that the parts in-scope of the request concerning documents 10, 13, 15 that were fully disclosed to the applicant; and documents 9 and 14 only contain redactions to prevent attributing the views expressed to specific parties, which is aligned with the EO's proposal for solution (see para 9 of the Recommendation). This was explained in our letter dated 3 June 2022.

<sup>7</sup> Documents 8, 12, 17. Please note that documents 5, 6, 7, 11, 12, 16, 18 only contain redactions to prevent attributing the views expressed to specific parties, which is aligned with your proposal for solution (see paragraph 9 of the Recommendation), as well as to prevent the disclosure of personal data (which is not challenged by the applicant). This was explained in our letter dated 3 June 2022.

<sup>8</sup> Documents 12 and 17. The application of Article 4(3)2nd paragraph of Regulation (EC) No 1049/2001 to document 8 only concerns redactions to prevent attributing the views expressed by specific parties, which is aligned with your proposal for solution (see paragraph 9 of the Recommendation).

For the first e-mail, while your Recommendation does not identify the specific document concerned, it maintains that the e-mail was not redacted on the basis of Article 4 Regulation (EC) No 1049/2001, but rather “to protect [the EDPB’s] internal process”. The EDPB Secretariat has identified one email that it believes could meet this description. In document 12, the EDPB Secretariat’s functional mailbox was redacted to avoid possible disruptions to its working methods, whereby this e-mail address is strictly used for communications between the EDPB members and its Secretariat. If that e-mail address became public, it would lead to very significant disruptions of the working methods of the EDPB, as this functional mailbox would likely become flooded with spam and e-mails from external parties. This would also likely lead to numerous duplicate e-mails being received, given that the EDPB already has a separate functional mailbox for correspondence with external senders.

Disclosing this internal functional mailbox address, which was created to be dedicated to correspondence with EDPB members, as well as the European Commission, would therefore mean the EDPB Secretariat would need more time to process incoming e-mails, leading to delayed responses to the EDPB members. Therefore, the EDPB considers that the redaction of this e-mail address is justified on the basis of Article 4(3) 2<sup>nd</sup> paragraph of Regulation (EC) No 1049/2001, as disclosure would severely hinder the EDPB Secretariat from performing its tasks in accordance with Article 75(6)(b) GDPR. The EDPB considers that there is no overriding public interest that could be relevant to disclose this internal e-mail address, as the EDPB has another functional mailbox specifically dedicated to exchanges with external parties, the address of the latter being public<sup>9</sup>.

For the second e-mail, your Recommendation provides an exact reference (“email of 09 February 2021 (18:59)”), which enabled the EDPB Secretariat to identify this as an e-mail in part of the e-mail chains in document 11. It was exchanged between two EDPB Secretariat staff members, hence falling outside of the scope of this access to documents request. The reasoning for this redaction was included in the replies to the initial<sup>10</sup> and confirmatory requests<sup>11</sup> in case 2021-37-C, and in the correspondence between the EDPB or its Secretariat and your Office<sup>12</sup>.

## 2. EDPB Response to the Ombudsman’s assessment

### 2.1. EDPB reliance on Article 4(3) of Regulation (EC) No 1049/2001

#### ***2.1.1. The risks to the independence of the EDPB and its members***

With regard to the documents partially disclosed, the EDPB considers that the exception under Article 4(3) 2<sup>nd</sup> paragraph of Regulation (EC) No 1049/2001 applies. In the following lines, the EDPB provides detailed arguments in order to explain, in the most precise way possible, its reliance on that exception and the specific and actual risks that disclosure would cause to its decision-making process.

---

<sup>9</sup> Letter from the EDPB Chair to the Ombudsman’s Director of Inquiries, 3 June 2022, p. 5.

<sup>10</sup> Letter of 18 January 2021 from the EDPB Vice-Chair.

<sup>11</sup> Letter of 9 February 2022 from the EDPB Chair.

<sup>12</sup> E-mail of 10 March 2022 from the EDPB Secretariat, and letter of 3 June 2022 from the EDPB Chair.

The EDPB fully agrees with and is committed to ensuring transparency of its decision-making process, in line with Articles 1 and 10 TEU and Article 15 TFEU. The EDPB concurs with the Ombudsman in that the principle of transparency applies to all documents held by EU institutions, bodies and agencies, as it “*guarantees that the administration enjoys greater legitimacy and is more effective and more accountable to the citizen*”<sup>13</sup>. The EDPB also acknowledges that such principle applies regardless of whether the documents form part of the EU’s legislative process<sup>14</sup>.

The EDPB underlines that, in cases where documents are part of the EU’s legislative process, the principle of transparency requires a wider access to the documents, which “*should be made directly accessible to the greatest possible extent*”<sup>15</sup>. The CJEU has emphasised this in consistent case law, where it recognised the importance of involving citizens in the decision-making process in the context of the legislative process by providing them with timely access to the information<sup>16</sup>. The EDPB highlights that the case law referred to in paragraph 24 of your Recommendation becomes relevant in the context of the legislative process. Indeed, both judgements quoted refer to final versions of internal documents used in the context of a legislative decision-making process<sup>17</sup>. On the contrary, the EDPB is a body with no legislative powers and the documents within the scope of your Recommendation are not final, but rather drafts containing track changes and internal comments made at staff level. Therefore, the findings made by the CJEU in T-144/05 and T-540/15 are not applicable *mutatis mutandis* to the case at hand. The EDPB had already provided partial access to the e-mails within the scope of the request, only redacting some parts whose disclosure would undermine its decision-making process<sup>18</sup>. In addition, and keeping in mind the Recommendation and the EDPB’s pursue of transparency, the EDPB decided to revisit its approach and disclose all the draft versions of Statement 04/2021, only redacting some of the internal comments made at staff level, in line with your proposal to anonymise the documents. By disclosing these documents, the EDPB believes that it provides the applicant with a clear overview of its decision-making process regarding the specific files, without it being necessary to disclose internal comments made by staff members in a draft document or an e-mail to achieve this goal.

In this respect, the EDPB wishes to reiterate that disclosure of internal comments containing views and opinions of staff members is not afforded since it could lead to the re-identification of the authors or, at the very least, the party(ies). This risk is not purely hypothetical but real, foreseeable and in fact, based on a previous recent experience: in the context of the Ombudsman Decision in case 386/2021/AMF, disclosure of internal comments where only the authors were anonymised did not

---

<sup>13</sup> The Recommendation, paragraph 16 and Regulation (EC) No 1049/2001, Recital 2.

<sup>14</sup> The Recommendation, paragraph 16.

<sup>15</sup> Recital 6 of Regulation (EC) No 1049/2001.

<sup>16</sup> Judgment of 4 September 2018, *ClientEarth v Commission*, [C-57/16 P](#), EU:C:2018:660, paragraph 84 and the case law cited therein.

<sup>17</sup> Judgment of 18 December 2008, *Pablo Muñiz v Commission*, [T-144/05](#), EU:T:2008:596, is about meeting minutes (paragraph 77); and judgment of 22 March 2018, *Emilio de Capitani v European Parliament*, [T-540/15](#), EU:T:2018:167, relates to multi-column tables used during the legislative decision-making process (paragraphs 1, 3-4).

<sup>18</sup> See footnote 9 above.

prevent the attribution of views to specific parties<sup>19</sup>. This will affect the EDPB's decision-making process as it can be used in an attempt to discredit the EDPB and/or some of its members and/or exert pressure over them. This is especially the case if we take into account the role of the EDPB members at national level as the competent supervisory authorities ("SAs") to ensure compliance with national and EU data protection rules, including the supervision of the Member States' compliance with their obligations. Given the fact that the redacted comments (including the ones made in the e-mails) portray opinions and views of national authorities - at staff level - with regard to documents addressing data protection compliance in the field of international agreements and administrative arrangements between public bodies, it is particularly important to ensure that SAs are able to fulfil their tasks in an independent manner and without being subject to any external pressure<sup>20</sup>, including from Member States' governments. Should the internal comments at issue be disclosed, the EDPB considers that there is a reasonably foreseeable risk that Member States' governments attempt to exercise pressure on their competent SA, especially considering that Statement 04/2021 invited Member States to assess and review their international agreements involving international transfers in light of the EU data protection framework, and the SAs' role in supervising compliance with data protection rules.

### **2.1.2. The risks to the EDPB's mission and the decision-making process**

The EDPB also wishes to underline its task of ensuring the consistent application of the GDPR and the LED<sup>21</sup>. In order to achieve such mission, it is essential that the EDPB speaks with one voice in accordance with its guiding principles of collegiality, inclusiveness and cooperation<sup>22</sup>. In this respect, the EDPB understands the added value of the draft documents for stakeholders in order to understand the process leading to the adoption of the final documents. The different draft versions are a result of the discussions, cooperation and agreements of the EDPB members during the decision-making process and reflect the different stages which the documents underwent. In this respect, the documents that the EDPB proposes to disclose already provide the public with a clear understanding of the decision-making process in the given case<sup>23</sup>, without jeopardising the EDPB's mission to speak with one voice.

---

<sup>19</sup> Please see for instance of the public allegations by some stakeholders following disclosure of draft guidelines 2/2019 following the Ombudsman Decision in case 386/2021/AMF: noyb, *noyb's Second "Advent Reading": How the Irish DPC tried to lobby Facebook's "GDPR bypass" into European Guidelines* (available at <https://noyb.eu/en/second-noyb-advent-reading-facebookdpc-documents>); Politico, *'Contrary to everything we believe in': Irish data watchdog lobbied for business-friendly GDPR* (available at <https://www.politico.eu/article/irish-data-protection-commission-gdpr-lobby-business-friendly-general-data-protection-regulation/>).

<sup>20</sup> Article 39 TEU; Article 16(2) TFEU; Article 8(3) EU Charter; Article 52 Regulation 2016/679 ("GDPR"); Article 42 Directive 2016/680 ("LED").

<sup>21</sup> Article 70 GDPR and Article 51(1)(b) LED. See also Article 2 of the EDPB's Rules of Procedure (available at [https://edpb.europa.eu/our-work-tools/our-documents/rules-procedure/rules-procedure-version-8\\_en](https://edpb.europa.eu/our-work-tools/our-documents/rules-procedure/rules-procedure-version-8_en)).

<sup>22</sup> Article 3 EDPB Rules of Procedure.

<sup>23</sup> In relation to the views expressed by the Ombudsperson under section 3 of the confidential annex to the Recommendation.

By contrast, the EDPB is of the view that its role will be undermined in the event that internal deliberations are made public. Indeed, the redacted comments contain opinions for internal use as part of deliberations and preliminary consultations within the EDPB whose disclosure would undermine the decision-making process of the EDPB<sup>24</sup>. Firstly, the EDPB underlines that the internal comments at hand were made during the drafting stage at staff level and do not necessarily reflect the official position of the concerned EDPB members. If staff members fear that internal comments expressed during deliberations may be made public, this could lead to the censoring of their own views and opinions<sup>25</sup>. In this regard, even if the internal comments were anonymised by redacting only the name of the individuals and/or of their SA, there is still a risk of re-identifying the SA of the staff member and, therefore, the concrete author of the comment could also be identified<sup>26</sup>. Likewise, the redaction of some parts of the e-mails at stake aims at addressing the risk of re-identification and attribution of a concrete view or opinion to the specific author or SA. This is a real, foreseeable and tangible risk which some EDPB members have already shared concerns about. This will undoubtedly have a very significant negative impact on the EDPB's deliberations during its decision-making processes. In this respect, the EDPB wishes to emphasise once again its working methods, whereby the EDPB members play an essential role in feeding the work of the EDPB. This is particularly the case in relation to guidelines, statements and other guidance, where the rapporteurs are usually SAs. In addition, in the context of the discussions in the dedicated expert subgroups, the EDPB members have a prominent role in providing written and oral comments, discussing options and reaching compromises. This is clearly reflected by the several draft versions of the statement within the scope of this case. Therefore, should some EDPB members censor sharing their views in preparatory work that is essential in the proper running of the EDPB, the risk that the EDPB is not able to fully achieve its tasks in the future, at least when it comes to drafting and adopting guidance, is reasonably foreseeable and not merely hypothetical<sup>27</sup>. This reasoning applies both with regard to documents 12, 17 and 23 of the present case, where the redactions aim at protecting the decision-making process when a decision has already been taken, as well as to document 8, where the redacted view concerns an issue for which a decision has not been taken yet by the EDPB.

Considering the above, and with the aim of fully complying with your Recommendation of providing the broadest possible access to the documents in an anonymised format, the EDPB decided to disclose all the drafts of Statement 04/2021 at issue, including those with track changes, and only redact the

---

<sup>24</sup> Judgment of 21 July 2011, *Sweden v MyTravel and Commission*, [C-506/08 P](#), EU:C:2011:496 paragraph 78; and judgment of 22 May 2012, *Internationaler Hilfsfonds v Commission*, [T-300/10](#), EU:T:2012:247, paragraph 131.

<sup>25</sup> Judgment of 15 September 2016, *Philip Morris v Commission*, [T-18/15](#), EU:T:2016:487, paragraph 87: "[...] *The possibility of expressing views independently within an institution helps to encourage internal discussions with a view to improving the functioning of that institution and contributing to the smooth running of the decision-making process*" (emphasis added).

<sup>26</sup> For example, the use of specific language or formulations can give an indication of the geographical location or mother tongue of the author of the comment, which could be an element to identify either the SA, or the author or both.

<sup>27</sup> Judgment of 22 May 2012, *Internationaler Hilfsfonds v Commission*, [T-300/10](#), EU:T:2012:247, paragraph 91 and 92 and case law cited therein.

information whose disclosure was essential to protect the fulfilment of its mission and its decision-making process.

Finally, the EDPB wishes to clarify its previous references to the need to preserve its independence<sup>28</sup>. The independence of the EDPB and its members is an essential element to enable the EDPB's task of ensuring the consistent application of the GDPR<sup>29</sup> and encouraging the consistent application of the LED<sup>30</sup>, as well as the SAs' task of monitoring the application of the GDPR<sup>31</sup> and of the provisions adopted pursuant to the LED<sup>32</sup>. In line with this, the EDPB Rules of Procedure establish the rules on confidentiality of the discussions in several situations, including when the EDPB decides so given the nature of the topic<sup>33</sup>. The EDPB fully agrees with the Ombudsman in that internal rules of procedure do not take legal precedence over a Regulation, and reassures that this was never the understanding nor intention of the EDPB. On the contrary, the EDPB fully abides by the obligation stemming from Regulation (EC) No 1049/2001 and the case law to demonstrate that the risks posed by the disclosure of the internal comments at hand are real, foreseeable and not purely hypothetical, in addition to demonstrating that there is no overriding public interest<sup>34</sup>. The independence of the EDPB and its confidentiality rules are mere elements stemming from the GDPR and the EDPB's Rules of Procedure which substantiate the EDPB's views that its decision-making process may be undermined by the disclosure of these internal comments, given the negative effect that it may have in the independence of the EDPB and its members. Thus, as explained above, the EDPB took these aspects into consideration when determining whether disclosure should be rejected on the basis of Article 4(3) of Regulation (EC) No 1049/2001.

### 3. Concluding remarks

In light of the above, we consider that the EDPB has sufficiently demonstrated a specific and actual risk to its decision-making, and the absence of an overriding public interest in disclosure of the internal comments.

To conclude, we would like to reiterate our intention to proactively apply the same approach as presented above, for future requests concerning revised versions of documents, where relevant, taking always into account the specificities of the request(s) assessed. We stand ready to review these arrangements regularly to ensure they remain fit for purpose.

As requested, we are enclosing a translation into French of this reply. Please note that in order to provide this reply within the deadline, only a machine translation could be provided. We trust that you will appreciate this sincere effort and the action, under our existing constraints. Considering that

---

<sup>28</sup> In relation to the views expressed by the Ombudsman in paragraphs 26-27 of the Recommendation.

<sup>29</sup> Articles 69-71 GDPR.

<sup>30</sup> Article 51(1)b) LED.

<sup>31</sup> Articles 51, 52 and 57 GDPR.

<sup>32</sup> Articles 41, 42 and 46 LED.

<sup>33</sup> Article 33 of the EDPB's Rules of Procedure.

<sup>34</sup> See section 2.1.3.



European Data Protection Board

the language of the complaint in Joint cases 509/2022 and 1698/2022 was English, please let us know should a formal translation be required.

We would like to conclude by reassuring you again that EDPB takes transparency matters very seriously, and will continue to do so in the future.

Yours sincerely,

Anu Talus

Chair of the EDPB

European Data Protection Board  
Rue Wiertz, 60  
1047 Brussels

# Letters



Moritz Körner  
Member of the European Parliament

By e-mail only

Brussels, 7 July 2023

Ref: OUT2023-0055

Dear Mr Körner,

Thank you for your letter of 09 November 2022 as regards your proposal on the possibility of establishing that all new laptops entering the EU market would need to be equipped with a physical camera cover based on Article 25 GDPR.

I would like to use this opportunity to reaffirm the position stated in the EDPB's letter of 16 June 2020 as follows:

The measures aimed at protecting and guaranteeing the rights and freedoms of natural persons must be established by the controller. Although manufacturers should be encouraged to take into account the right to data protection when developing and designing such products, services and applications, they are not responsible for the processing carried out with their products<sup>1</sup>. The GDPR does not provide for means to establish legal obligations on manufacturers, unless they also act as controllers or processors.

The GDPR does not specify any specific measure to fulfil the requirements of data protection by design and by default. Therefore, the controller shall choose the most appropriate measures according to the circumstances for the specific processing. As indicated in your letter, the physical camera cover is a tested, simple, cheap and efficient technology to prevent the camera from unduly collecting images. Nevertheless, there are other measures that could also be taken into consideration, *inter alia*, incorporating a physical on/off switch, or an easy way to deactivate the camera.

In addition, there are software solutions that can serve the same purpose and that give the control to the user. Nonetheless, the use of a software measure could present other associated risks, like bugs, introduction of unwanted "features" or the possibility of disabling the measure through remote access.

---

<sup>1</sup> Recital (78) GDPR.

To summarize, the objective of the controller shall be to provide sufficient guarantees to implement appropriate technical and organisational measures in such manner that the processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subjects. The controller shall choose the most appropriate measures for each specific processing according to the circumstances and following a risk assessment, in compliance with the GDPR.

Yours sincerely,

Anu Talus



Anu Talus  
Chair of the European Data Protection Board

rue Wiertz, 60  
1047 Brussels

# Letters



Moritz Körner  
Member of the European Parliament

By e-mail only

Brussels, 7 July 2023  
Ref: OUT2023-0056

Dear Mr Körner,

Thank you for your letter of 09 November 2022 as regards your concerns on the new 'private relay' function designed by Apple and its interaction with Article 25 GDPR.

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 data protection authorities. Thus, the following analysis is focused entirely on the application of the GDPR.

Article 25 GDPR provides for data protection by design and by default. This requires data controllers to have data protection designed into the processing of personal data and applied throughout the processing lifecycle. As a technology neutral legislation, GDPR does not imply any specific requirement in order to fulfil the conditions of its Article 25. Data controllers are accountable for choosing appropriate measures, given the circumstances for the specific processing. Hence, they are obliged to apply technical and organisational measures according to the principles of data protection by design and by default, while the choice of the concrete measures remains at their discretion.

The EDPB welcomes initiatives by controllers and providers of telecommunication services to minimise data processing in the course of the provision of their services, and limit the risks to the rights and freedoms of natural persons, regardless of whether they are intended to fulfil applicable requirements to implement data protection by design and default, or go beyond legal requirements. Obviously, those initiatives should not interfere with other legal obligations of the entities implementing them, nor should they introduce new risks that exceed the ones they intend to mitigate.

You have conveyed to the EDPB the concern of European network carriers that the private relay function introduced by Apple would prevent them from fulfilling their obligations under current legislative acts. Considering the available information the EDPB is not in the position to assess the fulfilment of any obligations that might be impeded by the implementation of a technical arrangement designed to encrypt and divert traffic via different proxy servers. In principle, neither the provisions

Anu Talus  
Chair of the European Data Protection Board

rue Wiertz, 60  
1047 Brussels

of the ePrivacy Directive, nor those of the GDPR affect or impede the fulfilment of legal obligations of controllers and providers of telecommunication services.

In fact, if controllers use new technology when processing personal data it raises specific obligations for controllers for example when the processing of personal data may carry high risk to the rights and freedoms of natural persons, to conduct a data protection impact assessment in line with Article 35 of the GDPR, and, when necessary, shall consult the competent supervisory authority prior to the commencement of processing of personal data in line with Article 36 of the GDPR.

Yours sincerely,

Anu Talus

Anu Talus  
Chair of the European Data Protection Board

rue Wiertz, 60  
1047 Brussels



European Data Protection Board

**Anu Talus**

Chair of the European Data Protection Board

Accredia  
Dr. Emanuele Riva  
Vice General Director

Brussels, 01 August 2023

*by e-mail only*

Ref: OUT2023-0061

***Subject: Reply to Accredia Letter [Ref: DC2023SPM054]***

Dear Dr. Riva,

Thank you for your letter of 3 May 2023, by which Accredia contacted the European Data Protection Board (“the Board” or the “EDPB”) in the context of the Europrivacy criteria of certification.

The Board appreciates your efforts to clarify the roles and competences of the different actors involved in certification and accreditation procedures under Regulation (EU) 2016/679 (“the GDPR”)<sup>1</sup>.

Please find below the approach of the EDPB regarding the different questions raised by Accredia.

---

<sup>1</sup> 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).

**Question 1 – Competence, adequacy, and effect of the EDPB Opinion**

We received a comment that “only the EU Commission owns the legal authority to establish mechanisms for the recognition of certification procedures, data protection seals and marks by means of implementing acts.” Could you clarify if this is the case and alternatively confirm that:

- a) **the EDPB is competent to adopt a European Data Protection Seal, without requiring the adoption of an implementing act by the EU Commission?**

Yes, the European Data Protection Board (EDPB) is competent to approve the criteria for a European Data protection seal, without the prior adoption of an implementing act by the European commission.

Pursuant to Articles 42 (5) and 70 (1) (o) of the General Data Protection Regulation ((EU) 2016/679 (GDPR)), the European Data Protection Board (EDPB) has the authority to approve the criteria of a certification scheme intended to be used in all EEA Member States: a European Data Protection Seal.

The authority of the EDPB to approve a European Data Protection Seal is not dependent on the prior adoption of a delegated or an implementing act of the European Commission (EC), pursuant to Articles 43(8) and (9) GDPR.

For instance, the Europrivacy certification criteria have been approved by the EDPB as European Data Protection Seal in its Opinion 28/2022<sup>2</sup>.

- b) **the GDPR and EDPB Guidelines allow for a scheme owner, like ECCP, to submit its certification criteria to Art. 42 GDPR without being itself an accredited certification body under Art. 43 GDPR?**

Yes.

The EDPB's Guidelines 7/2022 define a certification scheme owner as an identifiable organisation which has set up certification criteria and the requirements against which conformity is to be assessed<sup>3</sup>. The scheme owner may coincide with a certification body accredited pursuant to Art. 43(1) GDPR, but there is no requirement for the two entities to be same<sup>4</sup>.

---

<sup>2</sup> Opinion 28/2022 on the Europrivacy criteria of certification. Available at: <https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282022-europrivacy-criteria-certification>.

<sup>3</sup> Guidelines 07/2022 on certification as a tool for transfers (07.02.2023) p. 11. Available at: [https://edpb.europa.eu/system/files/2022-06/edpb\\_guidelines\\_202207\\_certificationfortransfers\\_en\\_1.pdf](https://edpb.europa.eu/system/files/2022-06/edpb_guidelines_202207_certificationfortransfers_en_1.pdf).

<sup>4</sup> EDPB Document on the procedure for the adoption of the EDPB opinions regarding national criteria for certification and European Data Protection Seals (2023) p. 2. Available at: [https://edpb.europa.eu/system/files/2023-02/edpb\\_document\\_procedure\\_for\\_the\\_adoption\\_edpb\\_opinions\\_regarding\\_national\\_criteria\\_for\\_certification\\_on\\_european\\_data\\_protection\\_seals\\_en.pdf](https://edpb.europa.eu/system/files/2023-02/edpb_document_procedure_for_the_adoption_edpb_opinions_regarding_national_criteria_for_certification_on_european_data_protection_seals_en.pdf).

It should be noted that a scheme owner seeking approval of its certification criteria must always apply to a supervisory authority (SA), regardless of whether the certification scheme is intended to become a European Data Protection Seal or is only valid nationally<sup>5</sup>.

For example, the Luxembourgish supervisory authority (LU SA), following its own assessment of the Europrivacy certification criteria drafted by the European Centre for Certification and Privacy (ECCP), submitted the Europrivacy certification criteria to the EDPB for approval, pursuant to 64 (2) GDPR, as a European Data Protection Seal. However, the approved criteria only become operational following accreditation of a certification body.

- c) the EDPB Opinion 28/2022 is not limited to provide guidance to the Luxembourgish supervisory authority, but it constitutes a formal decision by EDPB that is valid, effective, and applicable to all EU and EEA Members States?**
- d) The Europrivacy criteria have been formally approved to serve as European Data Protection Seal that can be used in all EU and EEA Member States.**

*Please note that the answer replies to both points c) and d).*

Yes, assuming that in relation to your question 1(d) you mean that the Europrivacy criteria have been formally approved to serve as *criteria* for a European Data Protection Seal that can be used in all EU and EEA Member States. It is important to note that the approved criteria are not identical to the data protection seal itself, since the criteria only become operational following the accreditation of a certification body.

According to Art. 42(5) GDPR, which refers to Art. 63 GDPR, the approval of a certification mechanism by the EDPB must follow the consistency procedure in Art. 64 GDPR.

As explained in the answer to question 1.b, when the competent SA receives an application for a certification mechanism intended to become a European Data Protection Seal, it will, after its assessment, refer the matter to the EDPB for an opinion, pursuant to Art. 64(2) GDPR.

Then, pursuant to Art. 64(3) GDPR, the EDPB will adopt an opinion that either approves or rejects that the certification criteria fulfil the requirements of the GDPR, interpreted in line with the EDPB Guidelines 1/2018 on certification<sup>6</sup>.

---

<sup>5</sup> EDPB Document on the procedure for the adoption of the EDPB opinions regarding national criteria for certification and European Data Protection Seals (2023) p. 2.

<sup>6</sup> Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation (Version 3.0), p. 36, available at:

[https://edpb.europa.eu/sites/default/files/files/file1/edpb\\_guidelines\\_201801\\_v3.0\\_certificationcriteria\\_anne\\_x2\\_en.pdf](https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_anne_x2_en.pdf);

Opinion 28/2022 on the Europrivacy criteria of certification regarding their approval by the Board as European Data Protection Seal pursuant to Article 42.5 (GDPR) (10.10.2022), pp. 3, and 25-27. EDPB Document on the procedure for the adoption of the EDPB opinions regarding national criteria for certification and European Data Protection Seals (2023) p. 34 and Annex A.

Therefore, following the adoption of EDPB's opinion 28/2022, the Europrivacy certification criteria can be applied in all EEA Member States, without any additional criteria, by certification bodies – accredited in compliance with Art. 43 GDPR by the respective competent NAB or SA – to conduct certification under these criteria<sup>7</sup>.

#### **Question 2 – Competent authority for delivering national accreditation under art. 43 GDPR**

**Could you confirm that the accreditation/agreement procedures under Art. 43 GDPR are performed in principle by the competent authority of the country where the certification body is located?**

Yes.

Accreditation for a European Data Protection Seal shall occur in the Member State where the certification body intending to operate the scheme has its' headquarters. Where other establishments or offices manage and perform certifications autonomously, each of these establishments or offices will require separate accreditation in the Member State where they are based<sup>8</sup>.

In other words, if a certification body wants to issue certificates in Member State, in line with Art. 43 (1) GDPR, the certification body has to become accredited in accordance with the requirements for accreditation adopted by the SA of that Member State, pursuant to Art. 43 (3) GDPR.

According to art. 43(1), the accreditation process of certification bodies may be conducted either by the SA or the national accreditation body (NAB) or both.

#### **Question 3 – Ability of EA to support Art. 43 GDPR Accreditation procedures**

**Can EA conduct a further and additional evaluation (fulfilling the EA-1/22 A 2020 requirements), to assess whether the Europrivacy scheme is an accreditable scheme under ISO/IEC 17065, in compliance with GDPR?**

The assessment conducted by the SAs and the EDPB for the approval of the certification criteria for a European Data Protection Seal focuses on whether the criteria are compliant with the GDPR, interpreted in line with Guidelines 1/2018. The scope of the EDPB Opinion 28/2022 does not cover the accreditability of the Europrivacy certification scheme under EN-ISO/IEC 17065.

It should be noted that the EDPB, in its internal procedure for handling applications for approving certification criteria, recommends SAs, that do not accredit certification bodies themselves, to collaborate with their NAB<sup>9</sup>. Whilst this is not a requirement that stems from the GDPR, it is encouraged by the EDPB to facilitate the accreditability of certification mechanisms.

As to the evaluation of the accreditability by the EA, the EDPB considers that it is outside its mandate to determine whether such an evaluation may take place or not. Nevertheless, the EDPB welcomes all

---

<sup>7</sup> Guidelines 1/2018, p.43.

<sup>8</sup> Guidelines 1/2018, p. 44.

<sup>9</sup> EDPB Document on the procedure for the adoption of the EDPB opinions regarding national criteria for certification and European Data Protection Seals (2023) p. 12.

initiatives aiming at harmonizing the approach adopted by NABs so as to ensure a consistent evaluation of the accreditation of European Data Protection Seals.

In this regard, the EDPB invites the EA to consider how the NAB that takes the lead for the assessment of the accreditation of a European Data Protection Seal could liaise with national SAs that perform accreditation of certification bodies, in accordance with Art. 43(1) (a) GDPR. The EDPB would also be open to exchange views and best practices with the EA, concerning the accreditation of certification mechanisms pursuant to the GDPR.

#### **Question 4 – European Cooperation in Accreditation Procedures**

- a) Can a National Accreditation Body, recognized by Reg. 765, accredit for a GDPR European scheme a certification Bodies not established in its country? For example, could Accredia accredit a certification body established in another country for the Europrivacy scheme, if the National Accreditation Body of the other country agrees with such approach?**
- b) If yes, should Accredia apply for this accreditation the national criteria established by Italian DPA, or the additional criteria established by the other country's Supervisory Authority?**

*Please note that the answer replies to both points a) and b).*

According to Art. 6 (3) of Reg. 765/2008: “national accreditation bodies shall be permitted to operate across national borders, within the territory of another Member State, either at the request of a conformity assessment body in the circumstances set out in Art. 7(1), or, if they are asked to do so by a national accreditation body in accordance with Art. 7(3), in cooperation with the national accreditation body of that Member State.”

The EDPB considers that the legal situation of cross-border accreditation of certification bodies within the scope of the GDPR is inconclusive<sup>10</sup> and would invite the EA to discuss the topic further. In this matter, the EDPB reiterates that the accreditation of a certification body for a European Data Protection Seal shall be granted in the Member State where the certification body that is intending to operate the certification scheme has its’ headquarters, or in the Member State where the certification body has other establishments or offices managing or performing certification autonomously. The competence over a certifying body is thus *not* dependent on where the accrediting NAB is located, which entails that the additional accreditation requirements that apply for the accreditation of the certification body are those approved by the certification body’s competent SA.

---

<sup>10</sup> The EDPB Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679) state that the fact that Art. 43 (1) GDPR allows accreditation by SAs is a derogation from the general principle that accreditation is to be conducted exclusively by NABs, means that the GDPR is *lex specialis* in relation to Art. 2(11) of Regulation (EC) 765/2008. See para. 33 of the Guidelines 4/2018 (Version 3.0). Available at:

[https://edpb.europa.eu/sites/default/files/files/file1/edpb\\_guidelines\\_201804\\_v3.0\\_accreditationcertification\\_bodies\\_annex1\\_en.pdf](https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertification_bodies_annex1_en.pdf).

### Question 5 – Possibility to Use Europrivacy for Voluntary Certifications

**Would it be possible to use the Europrivacy criteria on a voluntary basis, for assessing compliance of data processing activities and delivering certification outside of the scope of Art. 42 and 43 GDPR [in non-EEA jurisdictions]?**

No, the Europrivacy criteria as approved in Opinion 28/2022, the EuroPrivacy name, trade mark or brand and the approved EuroPrivacy Seal or any names or seals likely to be confused with it cannot be used for certification outside the scope of Art. 42 and 43 GDPR (see below), but this does not preclude the use of the Europrivacy criteria for self-assessment without any attestation of conformity.

First, it should be noted that GDPR certification pursuant to Articles 42 and 43 is a voluntary tool. Data controllers and processors are not required to hold a certification but they may use it as an element to demonstrate compliance with their obligations under the GDPR, as stipulated in Articles 24(3), 25(3), 28(5) and 32(3) GDPR. To that end, only certification criteria approved by a SA or the EDPB, may be relied upon to demonstrate compliance with the GDPR.

Accordingly, the use of certification criteria outside of the scope of Articles 42 and 43 GDPR would not have any of the legal effects anticipated by the GDPR. Whilst this does not preclude a controller or processor from using approved certification criteria as a tool for self-assessment of compliance with the GDPR, the data controller or processor could not in such a case refer to a certification, seal or mark as a certification pursuant to Articles 42 and 43 GDPR.

As to the Europrivacy certification criteria, it should be noted that the scope, as approved in Opinion 28/2022, is limited to controllers and processors established in the EU and the EEA. In this regard, the criteria cover – *inter alia* – obligations to assess compatibility with EEA Member State legislation complementary to the GDPR (cf. criteria G1.1.3 – National Regulation Compliance) and include requirements to notify competent SAs in certain situations, for example in case of a data breach (cf. criteria G7 – Management of data breaches). Hence, controllers or processors that are established outside the EU/EEA and outside the scope of the GDPR, are not in a position to comply with the entirety of the Europrivacy criteria and can therefore not obtain the Europrivacy European Data Protection Seal.

Finally, EDPB Guidelines 4/2018 clarify that data protection certificates, seals and marks “shall only be used” in compliance with Articles 42 and 43 GDPR and Guidelines 1/2018<sup>11</sup>. The purpose of this requirement is to ensure transparency and to enable other stakeholders and especially data subjects to quickly assess the level of data protection of relevant products and services provided by a certified controller or processor<sup>12</sup>. By contrast, the use of certification under the Europrivacy label outside the scope of the GDPR and the scope of the Europrivacy criteria approved in Opinion 28/2022, could create a situation of unfair competition, as entities certified under the label could be seen as having obtained a certification that demonstrates compliance with the GDPR. In the view of the EDPB, this

---

<sup>11</sup> Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679) (Version 3.0) Annex 1, section 4.1.3.

<sup>12</sup> Recital 100 GDPR.



European Data Protection Board

could jeopardise the validity of and trust in the system of accreditation and certification under the GDPR.

However, reusing some of the Europrivacy criteria within a certification mechanism outside the scope of application of GDPR would be possible, if such use is without prejudice to any other applicable law (including intellectual property rights). Additionally it shall be clearly stated that the use of the criteria results in a certification which is different from the EuroPrivacy name, trade mark or brand and the approved EuroPrivacy Seal or any names or seals likely to be confused with it. Lastly, it shall be clearly underlined that it is not a GDPR certification.

Yours sincerely

Anu Talus



European Data Protection Board

**Anu Talus**

Chair of the European Data Protection Board

Ms. Sophie in 't Veld  
Member of the European Parliament

Brussels, 04 October 2023

*by e-mail only*

Ref: OUT2023\_0073

***Subject: Your letter to the EDPB of 29 June 2023***

Dear Ms. in 't Veld,

I would like to thank you for your letter of 29 June 2023 concerning the amendments passed by the Irish Parliament on 28 June 2023 by way of the Courts and Civil Law (Miscellaneous Provisions) Bill 2022 and including rules on the confidentiality of data protection investigations.

Firstly, I would like to stress that the EDPB takes the question of confidentiality of procedures very seriously, particularly with regard to the proper functioning of the GDPR cooperation and consistency mechanism.

The EDPB has addressed the topic of confidentiality in its Guidelines 02/2022 on the application of Article 60 GDPR<sup>1</sup>. These Guidelines state:

*"The LSA and other CSAs may flag specific pieces of information as (highly) confidential, particularly when this seems necessary in order to meet requirements of confidentiality constraints laid down in national laws. In such a case, the SAs should inform each other immediately and jointly find legal options for a solution against the background that confidentiality provisions usually relate to external third parties and not to CSAs. In this regard, any information received that is subject to national secrecy rules should not be published or released to third parties without prior consultation with the originating authority, whenever possible."*

Therefore, the Guideline clarify that Lead Supervisory Authorities (LSAs) and Concerned Supervisory Authorities (CSAs) should jointly find solutions to confidentiality constraints, taking account that such constraints should not, as a rule, affect the cooperation procedure among SAs.

---

<sup>1</sup> EDPB Guidelines 02/2022 on the application of Article 60 GDPR, adopted on 14 March 2022.

In addition, on 10 October 2022, the EDPB sent a letter to the EU Commission, the annex of which contained a list of procedural aspects that could benefit from further harmonisation at EU level<sup>2</sup>. This was done with a view to ensuring the full effectiveness of the GDPR's cooperation and consistency mechanism ('the EDPB wish-list'). In this wish-list, the EDPB highlighted the need for further clarity on the rights of controllers, processors and complainants to receive documentation relating to the proceedings, and on how they can use the information received, including in the terms of disclosure.

On 4 July 2023, the European Commission issued a Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of the GDPR<sup>3</sup>—and formally consulted the EDPB and the EDPS jointly on that Proposal. The Proposal contains specific provisions in this respect to harmonise confidentiality requirements in cross-border proceedings. During its 84th Plenary on 19 and 20 September, the EDPB adopted an EDPB-EDPS Joint Opinion 01/2023 on the Proposal for a Regulation on procedural rules for the enforcement of the GDPR<sup>4</sup>.

The EDPB welcomes the Proposal for an EU-harmonised solution on this matter and expect this solution to foster cooperation amongst supervisory authorities. In this context, the Proposal highlights the importance for such solutions not to impair the exchange of information among supervisory authorities. The Proposal also takes into account the need to protect the confidentiality of sensitive information and to prevent disclosure that could negatively impact ongoing administrative or judicial proceedings.

Please be reassured that the EDPB takes the question of confidentiality of procedures very seriously and that we will continue to monitor the developments on this topic.

Yours sincerely,

Anu Talus

---

<sup>2</sup> [EDPB Letter to the EU Commission on procedural aspects that could be harmonised at EU level, issued on 10 October 2022](#).

<sup>3</sup> [Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation \(EU\) 2016/679](#).

<sup>4</sup> [EDPB-EDPS Joint Opinion 01/2023 on the Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation \(EU\) 2016/679](#)

**Anu Talus**  
Chair of the European Data Protection Board

Sophie in't Veld  
Member of the European Parliament  
Rue Wiertz, 60  
B-1047 Brussels  
Belgium

Brussels, 25 September 2023

*by e-mail only*  
Ref: OUT2023-0074

***Subject:***

Dear Ms in't Veld,

I wish to thank you for your letter of 6 April 2023, in which you raise questions on measures taken by the EDPB following the Ombudsman's recommendation of 29 March 2023 in case 201/2022/JK, as well as on the enforcement of the GDPR in relation to the transfers of personal data carried out on the basis of intergovernmental agreements (IGAs) implementing the US Foreign Account Tax Compliance Act (FATCA).

With regard to your first question in relation to the European Ombudsman ("EO")'s Recommendation of 29 March 2023 in case 201/2022/JK, the EDPB decided to follow such Recommendation and provided broadest possible access to the preparatory documents covered by the underlying complaint. The EDPB's detailed response sent to the EO on this matter on 28 June 2023 is available on our website<sup>1</sup>.

As regards your second and third questions on the role of the EDPB in the enforcement of data protection rules by national supervisory authorities (SAs) on FATCA, I would like to stress that the task of monitoring and, where necessary, enforcing compliance of IGAs with the GDPR concluded bilaterally between a Member State and the United States does not fall within the competence of the EDPB. In accordance with Articles 55 and 57(1)(a) GDPR, the enforcement of data protection law in respect of these IGAs is the sole responsibility of national SAs in their respective jurisdictions, for which the EDPB has no supranational powers.

While it is up to each SA to monitor the review of these IGAs and the EDPB is limited in the updates it can provide in order not to jeopardise actions taking place at national level, I would like to reassure

---

<sup>1</sup> EDPB Response to the European Ombudsman's recommendation regarding case 201/2022/JK, available at [https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-response-european-ombudsmans-recommendation-regarding\\_en](https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-response-european-ombudsmans-recommendation-regarding_en).



European Data Protection Board

you that, as part of its tasks under Article 70 GDPR, the EDPB dedicates special attention to this matter. In particular, the EDPB (and previously WP29) has dealt on several occasions with the transfers of personal data based on the intergovernmental agreements of the Member States, including FATCA<sup>2</sup>. Building on these initiatives, and pursuant to Article 70(1)(u) GDPR, the EDPB also promotes regular exchanges between its members in order to share information and best practices on the actions taken by supervisory authorities at national level with regard to transfers of personal data on the basis of these IGAs.

Although the EDPB cannot provide you with more detailed information on the progress of the ongoing investigations at national level, I would like to assure you that a number of steps have been taken by several SAs to engage with a dialogue with their respective ministries, in some cases on the basis of the complaints they have received. Also, the Belgian supervisory authority recently adopted a decision prohibiting the transfer of tax data of a Belgian complainant to the United States, in which it found that the data processing carried out under the FATCA agreement does not comply with all the principles of the GDPR, including the rules on data transfers outside the EU<sup>3</sup>.

Yours sincerely,

Anu Talus

---

<sup>2</sup> See 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 (<https://ec.europa.eu/newsroom/article29/items/640466>), and EDPB Statement 04/2021 on international agreements including transfers ([https://edpb.europa.eu/system/files/2021-04/edpb\\_statement042021\\_international\\_agreements\\_including\\_transfers\\_en.pdf](https://edpb.europa.eu/system/files/2021-04/edpb_statement042021_international_agreements_including_transfers_en.pdf));

<sup>3</sup> APD, Decision 61/2023 on the complaint relating to the transfer by the Federal Public Service Finance of personal data to the US tax authorities pursuant to the "FATCA" agreement, adopted on 24 May 2023. The decision is available at <https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-61-2023.pdf>. This decision makes specific reference to the EDPB Statement 04/2021.



European Data Protection Board

**Anu Talus**

Chair of the European Data Protection Board

Mr Fabien Lehagre

President of the Association des Américains Accidentels

Mr Vincent Wellens

NautaDutilh

Brussels, 30 November 2023

*by e-mail only*

Ref: OUT2023-0085

Dear Mr Lehagre,

Dear Mr Wellens,

Thank you for your letter of 13 April 2023, in which you articulate your concerns regarding transfers of personal data based on intergovernmental agreements (IGAs) implementing the US Foreign Account Tax Compliance Act (FATCA).

In your letter, you draw my attention to the different approaches adopted at national level on the compatibility of transfers carried out on the basis of these IGAs with the GDPR. In light of this, you request the EDPB to evaluate the assessment made by EU/EEA Member States of their FATCA agreements in relation to the GDPR. On this point, you refer specifically to the EDPB's invitation to Member States in its statement 4/2021<sup>1</sup> to assess and, where necessary, review their international agreements that involve international transfers of personal data.

In response to your concerns, allow me to emphasize that, according to the GDPR, the EDPB does not possess supervisory powers that enable it to compel Member States to review the various IGAs implementing FATCA in relation to the GDPR. In accordance with Articles 55 and 57(1)(a) of the GDPR, the application of data protection law in relation to IGAs implementing FATCA is the sole responsibility of national data protection authorities (DPAs) in their respective jurisdictions. The EDPB, whose competence to monitor and ensure the correct application of the GDPR is limited to the cases provided for in Articles 64 and 65, has no supranational powers in this respect.

Nonetheless, as part of its task under Article 70 GDPR, and building upon its previous positions (and its predecessor's, the WP29) concerning automatic exchanges of personal data for tax purposes,

---

<sup>1</sup> EDPB Statement 04/2021, available at: [https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-042021-international-agreements-including\\_en](https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-042021-international-agreements-including_en).



European Data Protection Board

including FATCA<sup>2</sup>, the EDPB is dedicated to foster regular information sharing and the exchange of best practices among its members regarding ongoing investigations. This collaborative approach aims to facilitate a consistent approach from the DPAs, as appropriate, on this matter.

In addition, you may have already noted the ongoing investigations being conducted by some national DPAs following AAA letters. While the EDPB is limited in the updates it can provide on these investigations in order not to compromise ongoing actions at national level, I would like to assure you that the Board, together with the national SAs that constitute it, are devoting particular attention to the interplay between the obligations arising from IGAs implementing FATCA and the GDPR.

Yours sincerely,

Anu Talus

---

<sup>2</sup> See 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 (<https://ec.europa.eu/newsroom/article29/items/640466>), and EDPB Statement 04/2021 on international agreements including transfers ([https://edpb.europa.eu/system/files/2021-04/edpb\\_statement042021\\_international\\_agreements\\_including\\_transfers\\_en.pdf](https://edpb.europa.eu/system/files/2021-04/edpb_statement042021_international_agreements_including_transfers_en.pdf));

**Anu Talus**

Chair of the European Data Protection Board

Marek Černoch

President of the Czech Association Companies  
of Financial Advice and Intermediation

Brussels, 30 November 2023

*by e-mail only*

Ref: OUT2023-0086

Dear Sir,

Thank you for your letter of 17 March 2023 to the EDPB regarding the interplay between the GDPR and Directive 2014/65/EU ('Directive MiFID II').

In your letter, you refer to questions raised in relation to the interplay between these two legislative texts in light of recommendations provided by the Czech National Bank.

The EDPB appreciates the importance of the points raised by the Czech Association Companies of Financial Advice in relation to Article 16(6) and (7) of the Directive MiFID II, and is grateful for the provided analysis. However, while I understand the importance of seeking guidance on this matter, I would like to clarify that the EDPB does not possess the same competence, tasks, and powers as national supervisory authorities. In accordance with Article 70(1)(a) GDPR, the EDPB's mission to monitor and ensure the correct application of the GDPR is limited to the cases provided for in Articles 64 and 65 GDPR.

Conversely, the responsibility for addressing compliance with data protection law falls under the jurisdiction of the respective national data protection authorities (DPAs) in each EU member state. Given the implementation of MiFID II may vary across member states, I therefore encourage you to direct your request to the Czech Supervisory Authority competent for data protection (Úřad pro ochranu osobních údajů), which will be in the best position to advise you on this matter.

At the same time, I would like to reassure you that the EDPB remains concerned about the need to ensure a consistent application of the GDPR within the European Union, including with regard to the interplay with MiFID II, and, in this context, thank you for bringing these matters to my attention.

Yours sincerely,

Anu Talus

**Anu Talus**  
Chair of the European Data Protection Board

European Payments Council AISBL  
Cours Saint-Michel 30  
B-1040 Brussels  
Belgium

Brussels, 30 November 2023

*by e-mail only*  
Ref: OUT2023-0087

Dear Sir or Madam,

I would like to thank you for your letter dated 28 February 2023, in which you sought advice from the EDPB regarding the sharing of personal data within a platform dedicated to threat intelligence and fraud-related information pertaining to payments.

In this respect, allow me first to reiterate that the EDPB has the general responsibility of ensuring the consistent application of the GDPR under Article 70(1) GDPR. In pursuit of this objective, the EDPB has previously issued Guidelines on the interplay between the GDPR and the revised Payment Services Directive (PSD2)<sup>1</sup>.

The EDPB has, in these Guidelines, provided its perspective that processing activities for the purpose of fraud prevention should be evaluated on a case-by-case basis by the data controller, in accordance with the principle of accountability<sup>2</sup>. In this regard, the EDPB would like to underscore that while the processing of personal data necessary for fraud prevention may be considered a legitimate interest of the payment service provider, the sharing of such personal data pertaining to fraud must be strictly limited and be provided by a clear and specific legal framework.

In this context, however, national data protection authorities (DPAs), in line with their responsibilities to promote awareness among controllers and processors of their obligations under the GDPR as stated in Article 57(1)(d) GDPR, are best placed to provide payment service providers with additional information and clarifications on the practical implementation of the aforementioned Guidelines. Hence, we encourage you to reach out to your competent national DPA should you require further guidance.

---

<sup>1</sup> EDPB Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR, 15 December 2020, available at: [https://edpb.europa.eu/our-work-tools/our-documents/guidelines-guidelines-062020-interplay-second-payment-services\\_en](https://edpb.europa.eu/our-work-tools/our-documents/guidelines-guidelines-062020-interplay-second-payment-services_en)

<sup>2</sup> Ibid, paragraph 20.



European Data Protection Board

Finally, I would like to assure you that the EDPB remains committed to ensuring continued efforts for a consistent interpretation of the GDPR including in the context of its interplay with PSD2, and is dedicated to extending these efforts to the new legislative proposal on PSD3.

Yours sincerely,

Anu Talus



European Data Protection Board

**Anu Talus**  
Chair of the European Data Protection Board

Mr Moritz Körner  
Member of the European Parliament

Brussels, 15 December 2023

*by e-mail only*

Ref: OUT2023-0099

***Subject: Your letter to the EDPB of 9 November 2022***

Dear Mr Körner,

Thank you for your letter of 9 November 2022 which contained your questions about the ‘Do Not Track’ function in Internet browsers and the related use of Article 21(5) GDPR. In this letter, we will also refer to the equivalent provision under Article 23(3) Regulation 2018/1725.

As a preface to our answer, the EDPB recalls that, under Article 5(3) Directive 2002/58/EC ('ePrivacy Directive') and in line with the CJEU's judgment in C-673/17 *Planet49 GmbH*, a website operator is only permitted to use cookies that are not strictly necessary (including those used for tracking) where the user has actively consented to their use. The concept of consent is defined under the Article 4(11) GDPR and requires a ‘freely given, specific, informed and unambiguous indication of a data subject’s wishes’. These elements have also been interpreted by, *inter alia*, the EDPB Guidelines 05/2020 on consent<sup>1</sup>. The EDPB also notes that, should a data subject wish to withhold their consent, there is no legal requirement for the data subject to ‘object’ to the request *per se*; rather, in such cases, the data subject simply does not provide their consent. Equally, Article 7(3) GDPR notes that data subjects ‘shall have the right to withdraw [their] consent at any time’ [emphasis added]. If, therefore, a data subject had previously given their consent but has now changed their mind, this would be effected by withdrawing that consent and not through an objection to the processing under Article 21(1) GDPR.

The EDPB further recalls that the material scope of the right to object is set out by Article 21(1) and (2) GDPR. Of these provisions, Article 21(1) GDPR only applies to processing which is necessary for the performance of a task carried out in the public interest under the Article (6)(1)(e) GDPR or to processing which is necessary for a legitimate interest under Article 6(1)(f) GDPR. Meanwhile, Article 21(2) GDPR is focused on processing performed for the purposes of direct marketing.

---

<sup>1</sup> EDPB Guidelines 05/2020 on consent under Regulation 2016/679, version 1.1 adopted on 4 May 2020, available at: [https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679\\_en](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en)



European Data Protection Board

While Article 21(5) GDPR may, therefore, be relevant to certain tracking activities, the EDPB notes that this provision should not be read as imposing a general requirement that website operator respect a user's Do Not Track settings. Further, a website operator wishing to use cookies which are not strictly necessary (including tracking cookies) should still take the required steps to actively obtain consent from users whose Do Not Track flag is set to permit tracking.

Regarding enforcement actions, the EDPB is aware that some complaints have been dealt with regarding websites' failure to respect Do Not Track signals. However, these have been dealt with as part of allegations of no or invalid consent, rather than under Article 21(5) GDPR or Article 23(3) Regulation 2018/1725, and the EDPB is not aware of any enforcement actions under either Article 21(5) GDPR or Article 23(3) Regulation 2018/1725 which relate to the Do Not Track function in Internet browsers *per se*. In this context, the EDPB also emphasises the importance of Article 5(3) ePrivacy Directive and notes the importance of the elements discussed above for future approaches to enforcement. Nevertheless, it is important to note that some supervisory authorities do encourage controllers to respect Do Not Track flags, and the European Data Protection Supervisor noted that respecting such flags, when set to not permit tracking, was a requirement for websites of EU Institutions and Bodies.

Finally, the EDPB would like to take this opportunity to reiterate our commitment to the protection of data subject rights. Thank you again for your letter and the EDPB sends its apologies for the delay in our response.

Yours sincerely,

Anu Talus



European Data Protection Board

**Anu Talus**

Chair of the European Data Protection Board

Ms Gallego  
Directorate-General for Justice and Consumers  
European Commission  
1049 Brussels

Brussels, 13 December 2023

by e-mail only

Ref: OUT2023-0098

***Subject: EDPB reply to the Commission's Initiative for a voluntary business pledge to simplify the management by consumers of cookies and personalised advertising choices – DRAFT PRINCIPLES (Ref. Ares(2023)6863760)***

Dear Ms Gallego,

Thank you for your letter of 10 October 2023, regarding the initiative for the voluntary cookie pledge launched by Commissioner Reynders, and for requesting the EDPB's views on the draft pledge principles.

The EDPB welcomes the Commission's initiative to gather stakeholders and promote discussions and exchanges of views on the use of cookies and any other systems used for tracking users' online navigation. The EDPB supports actions that aim at simplifying the management by users<sup>1</sup> of cookies and personalised advertising choices and empowering users' control over their personal data and privacy, in compliance with the GDPR<sup>2</sup> and ePrivacy Directive.<sup>3</sup>

In the view of the EDPB, the aim of the initiative should be to help protect the fundamental rights and freedoms of users, empower them to make effective choices, and provide a platform for stakeholders to exchange views. While voluntary commitments may be a useful tool, the pledging principles should by no means be used to circumvent legal obligations. In addition, undertaking voluntary commitments does not equate or guarantee compliance with the applicable data protection and privacy framework. They are without prejudice to the exercise of supervision and enforcement powers of competent national authorities, including authorities competent to supervise compliance with the national

---

<sup>1</sup> References in this letter and its annex to "users" and "data subjects" are interchangeable.

<sup>2</sup> OJ L 119, 4.5.2016, p. 1–88.

<sup>3</sup> OJ L 201, 31.7.2002, p.37, as amended by OJ L 337, 18.12.2009, p. 11–36.



European Data Protection Board

implementation law(s) of the ePrivacy Directive and authorities competent to supervise compliance with the GDPR.<sup>4</sup>

The EDPB understands from your letter that more work is needed to propose pledge principles that would allow a majority of interested parties to adhere to them. For this reason, the EDPB considers it useful to draw your attention to relevant guidance of the EDPB, and its predecessor the Article 29 Working Party, referred to in the Annex to this letter to inform your further work on the draft principles.

The EDPB remains available to continue assisting you further in the development of these pledge principles with a view to simplifying the management by users of cookies and similar technologies and personalised advertising choices while empowering users, in full compliance with the GDPR and ePrivacy Directive.

Yours sincerely,

Anu Talus

---

<sup>4</sup> The EDPB does not address any specificities of national implementation laws of Article 5(3) ePrivacy Directive in this letter. In addition, the EDPB notes that it has not consulted national competent authorities responsible for the supervision of the national implementation laws of the ePrivacy Directive that are not a supervisory authority pursuant to Article 51 GDPR.

## ANNEX - FEEDBACK ON THE COOKIE PLEDGE DRAFT PRINCIPLES

In this Annex, the EDPB provides remarks to inform the further work on the draft principles. Where relevant, the EDPB's remarks and analysis of certain draft principles is grouped together. The EDPB's observations on any of the draft principles, or lack thereof, should not be understood as endorsement. In addition, the EDPB's feedback on the draft principles should not be understood as endorsement of the use of cookies for purposes of behavioural or personalised advertising, which may be highly intrusive and raise additional legal issues, even if conducted in adherence with the principles. Supervisory authorities maintain the prerogative to assess individual cases and exercise their powers if necessary. The EDPB takes the view that a case by case analysis remains necessary to assess whether access or storage of information in terminal equipment and subsequent processing of such information is compliant with the ePrivacy Directive, as implemented in national laws, and with the GDPR.

### 1 GENERAL REMARKS

The EDPB understands from the Commission's letter that the cookie pledge voluntary initiative refers to cookies and any other systems tracking users' online navigation. Considering that the monitoring of online (and potentially offline) behaviour may take place via different tools,<sup>1</sup> the EDPB welcomes that the scope of the initiative is broader than cookies used for online behavioural or personalised advertising.<sup>2</sup> The EDPB shall therefore in its analysis refer to access and storage of information in terminal equipment in accordance with Article 5(3) ePrivacy Directive, irrespective of the technology used to store or gain access to that information.

The EDPB shall in its feedback of the draft principles not analyse all requirements to obtain valid consent in accordance with Article 4(11) and 7 GDPR. It would however like to highlight certain requirements for consent for access and storage of information in terminal equipment to be valid that do not seem to be reflected in the draft principles, namely:

- 1) data subjects must express their consent with an affirmative action. For example, the mere continuation of browsing a website or the use of general browser settings allowing the use of cookies do not constitute consent;
- 2) where consent is required, no access or storage of information in terminal equipment must take place before valid consent is obtained; and
- 3) data subjects must be able to withdraw their consent at any time, withdrawing consent must be as easy as giving consent, and data subjects must be informed of how to withdraw consent when asked to give their consent.

---

<sup>1</sup> See in this respect e.g. EDPB [Guidelines 2/2023 on Technical Scope of Art. 5\(3\) of ePrivacy Directive](#), adopted on 14 November 2023; Article 29 Working Party [Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting](#), adopted on 25 November 2014; and Article 29 Working Party [Opinion 2/2010 on online behavioural advertising](#), adopted on 22 June 2010.

<sup>2</sup> The EDPB recommends to clearly reflect the scope in the draft principles, which as currently drafted appear exclusively focussed on the use of cookies as such. This is the more pertinent considering technological developments and the ongoing discussion on the phasing out of third party cookies.

Furthermore, the EDPB emphasizes the information requirement. The information given to users on the access and storage of information in terminal equipment and the processing of personal data at the time consent is sought, is of paramount importance to ensure that a valid consent can be obtained.

Finally, the EDPB also recalls the *lex generalis – lex specialis* relationship between the GDPR and Article 5(3) ePrivacy Directive, which the EDPB has explained in several Opinions and Guidelines.<sup>3</sup>

## 2 DRAFT PRINCIPLE A

*A. The consent request will not contain information about the so-called essential cookies nor the reference to collection of data based on legitimate interest.*

As essential cookies do not require consent, not showing information about them in the context of the request for consent will reduce the information that users need to read and understand. In addition, legitimate interest is not a ground for data processing based on Article 5(3) of the ePrivacy Directive so it should not be included in the cookie banner. Where applicable, the issue of subsequent processing of data based on legitimate interest should be explained in the privacy notice.

### 1) Information regarding ‘essential’ cookies

The controller must, in accordance with Articles 12-14 GDPR, inform the user of the processing of personal data that is accessed or stored in terminal equipment. This requirement applies to access or storage of information for purposes that do and do not require consent under Article 5(3) ePrivacy Directive. The EDPB agrees, however, that detailed information on the use of strictly necessary cookies that are exempt from consent under Article 5(3) ePrivacy Directive should be presented distinct from a consent request (for which only information relevant to the consent request should be provided). The EDPB refers to the Guidelines on transparency under Regulation 2016/679<sup>4</sup> for further guidance.

Taking into account the above, the EDPB recommends clarifying in draft principle A that it remains necessary to provide users with information in accordance with Articles 12-14 GDPR whenever personal data are processed, even if the access or storage of information in terminal equipment does not require consent under Article 5(3) ePrivacy Directive. Information about the processing of personal data via the use of strictly necessary cookies could for example be accessible via a link on the first layer of the cookie banner, directing to the relevant section in the privacy policy, or the information could be provided on the second layer of the cookie banner, provided that the requirements of Articles 12-14 GDPR are complied with.<sup>5</sup>

The EDPB notes that the notion of “essential cookies” used in draft principle A may be misunderstood to cover more purposes than the two narrowly defined purposes which are exempt from the obligation to obtain consent pursuant to Article 5(3) ePrivacy Directive. As mentioned in the report of the Cookie

<sup>3</sup> See for example EDPB [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](#), paragraph 40. See also EDPB [Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications](#), adopted on 9 March 2021, paragraph 14; and EDPB [Report of the work undertaken by the Cookie Banner Taskforce](#), adopted on 17 January 2023, paragraphs 1-3.

<sup>4</sup> Article 29 Working Party [Guidelines on transparency under Regulation 2016/679](#), adopted on 29 November 2017, last Revised and Adopted on 11 April 2018. See also Article 29 Working Party Working [Document 2/2013 providing guidance on obtaining consent for cookies](#), adopted on 2 October 2013, p. 3.

<sup>5</sup> In this regard, see also Article 29 Working Party [Guidelines on transparency under Regulation 2016/679](#), paragraph 27, regarding the timing for the provision of information.

Banner Taskforce, some controllers may incorrectly classify certain cookies and processing operations as “essential” or “strictly necessary”, which would not be considered as such within the meaning of Article 5(3) ePrivacy Directive, or under GDPR.<sup>6</sup> The EDPB therefore recommends changing the term “essential” to “strictly necessary” within the meaning of Article 5(3) ePrivacy Directive. For more information on “strictly necessary” cookies, the EDPB refers to Opinion 04/2012 on Cookie Consent Exemption.<sup>7</sup>

## 2) No reference to ‘to collection of data based on legitimate interest’

The EDPB agrees that users should not be presented with information ‘referring to collection of data based on legitimate interest’ in the cookie banner, as this is not a valid legal basis under the ePrivacy directive for access or storage of information (including collection of data) in terminal equipment.<sup>8</sup>

In addition, the EDPB recalls that consent under Article 6(1)(a) GDPR will generally be the most adequate legal basis for the processing of personal data that takes places after access or storage thereof in terminal equipment based on consent under Article 5(3) ePrivacy Directive.<sup>9</sup> To avoid misunderstanding, the EDPB recommends stating this in Principle A.

## 3 DRAFT PRINCIPLES B, C, AND D

*B. When content is financed at least partially by advertising it will be explained upfront when users access the website/app for the first time.*

From the moment a business obtains revenues either i) by exposing consumers to tracking-based advertising by collecting and using information about consumers’ online behaviour through trackers or ii) by selling to partners the right to put trackers on consumer’s devices through their website, the consumers need to be informed of the business model in question at least at the same time as when cookie consent is required. Asking consumers to read complex cookie banners and only after they did not consent confronting them with a “pay or leave” ultimatum, could be considered manipulative.

*C. Each business model will be presented in a succinct, clear and easy to choose manner. This will include clear explanations of the consequences of accepting or not-accepting trackers.*

Most cookies are used to implement a business model and therefore this concomitance should be easily described, understood and implemented in one joint panel regrouping the agreements under consumer law and consent under the e-Privacy/GDPR law. In this panel, the business model options (i.e. accepting advertising based on tracking, accepting other types of advertising or agreeing to pay a fee) will be presented together with the consequences in terms of the purpose of trackers, and this in plain and simple language.

*D. If tracking based advertising or paying a fee option are proposed, consumers will always have an additional choice of another less privacy intrusive form of advertising.*

<sup>6</sup> EDPB [Report of the work undertaken by the Cookie Banner Taskforce](#), adopted on 17 January 2023, paragraph 26.

<sup>7</sup> Article 29 Working Party [Opinion 04/2012 on Cookie Consent Exemption](#), adopted on 7 June 2012.

<sup>8</sup> EDPB [Report of the work undertaken by the Cookie Banner Taskforce](#), adopted on 17 January 2023, paragraph 24.

<sup>9</sup> See e.g. EDPB [Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications](#), adopted on 9 March 2021, paragraphs 14-15. See similarly also EDPB [Report of the work undertaken by the Cookie Banner Taskforce](#), adopted on 17 January 2023, para.1-2.

In view of the extremely limited number of consumers who accept to pay for online content of various sorts and as consumers may navigate tens of different websites daily, asking consumers to pay does not appear a credible alternative to tracking their online behaviour for advertising purposes that would legally require to obtain consent.

The EDPB supports the objective of draft principles to enhance transparency on the business models used by stakeholders and to promote advertising models that are less intrusive than behavioural advertising. However, the EDPB highlights that beyond the consumer perspective, special attention should be paid to the protection of the terminal equipment as provided for by Article 5(3) ePrivacy Directive.

Draft principles B-D relate to the provision of valid consent under Article 5(3) ePrivacy Directive in conjunction with Article 4(11) and Article 7 GDPR, more in particular whether consent is freely given and informed, and will therefore be discussed together.

With regard to valid consent, the EDPB Guidelines 05/2020 clarify that in order to determine whether consent is freely given, it must be taken into account whether:

- i. there is any imbalance of power between the controller and data subject;<sup>10</sup>
- ii. consent is conditional, e.g. whether consent is “bundled” with acceptance of terms or conditions;<sup>11</sup>
- iii. consent is granular and is asked for each individual purpose;<sup>12</sup> and
- iv. it is possible to refuse or withdraw consent without detriment.<sup>13</sup>

Consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences (e.g. substantial extra costs) if they do not consent. Consent will not be free in cases where there is any element of compulsion, pressure or inability to exercise free will.<sup>14</sup> These elements must among others be taken into account when consent for access or storage of information in terminal equipment used for tracking based advertising is asked.

The EDPB also explained in Guidelines 05/2020 which elements of information are at a minimum required to obtain valid consent.<sup>15</sup> The EDPB agrees with the concepts enshrined in principles B and C stating that the user must be provided with clear information at the moment consent is sought. Moreover, the provided information about alternative models/services to the provision of consent to the access or storage of information in terminal equipment for advertising purposes may serve as a relevant factor when assessing whether consent for access or storage of information in terminal equipment is valid. At the same time, the EDPB notes that ‘information on the business models’ could be understood in different ways and recalls that it may not substitute information obligations

---

<sup>10</sup> EDPB [Guidelines 05/2020 on consent under Regulation 2016/679](#), adopted on 4 May 2020, paragraphs 16-24.

<sup>11</sup> EDPB [Guidelines 05/2020 on consent under Regulation 2016/679](#), adopted on 4 May 2020, paragraph 26.

<sup>12</sup> EDPB [Guidelines 05/2020 on consent under Regulation 2016/679](#), adopted on 4 May 2020, paragraphs 42-44.

<sup>13</sup> EDPB [Guidelines 05/2020 on consent under Regulation 2016/679](#), adopted on 4 May 2020, paragraph 46.

<sup>14</sup> EDPB [Guidelines 05/2020 on consent under Regulation 2016/679](#), paragraph 24.

<sup>15</sup> EDPB [Guidelines 05/2020 on consent under Regulation 2016/679](#), adopted on 4 May 2020, paragraph 64: i. the controller’s identity; ii. the purpose of each of the processing operations for which consent is sought; iii. what (type of) data will be collected and used; iv. the existence of the right to withdraw consent; v. information about the use of the data for automated decision-making in accordance with Article 22 (2)(c) where relevant; and vi. information on the possible risks of data transfers due to absence of an adequacy decision and of appropriate safeguards as described in Article 46.

regarding access or storage of information in the terminal equipment and on the processing of personal data.

The EDPB notes that a business model using contextual advertising is not mentioned in draft principle B as means for a business to obtain revenue. Such business model may involve the accessing or storing of information in terminal equipment and the processing of personal data, although generally much more limited than a business model that relies on the tracking of users and presenting them with behavioural or personalised advertising. The EDPB considers that just as for the business models currently referred to in draft principle B, users should be informed of a business model using contextual advertising at least at the same time as when they are requested for consent for the use of cookies, and therefore recommends that the type of advertising used is explained clearly (e.g. behavioural or contextual advertising). In other words, the EPDB recommends to also make reference to contextual advertising in principle B.

Draft principle C provides as alternative to advertising based on tracking “accepting other types of advertising”. Draft principle D refers to “another less privacy intrusive form of advertising”. The EDPB understands in this context that services that use the mentioned types/forms of advertising are not offered for a fee and recommends to explicitly clarify this in the principles. The EDPB recommends adding to both draft principles (C and D) a reference to contextual advertising as an example of another type/form of advertising, where such a business model is being operated.

The EDPB recalls that controllers that are gatekeepers pursuant to the Digital Markets Act<sup>16</sup> must comply with the respective requirements regarding the offering of alternative services. Recital 36 of the Digital Markets Act provides that gatekeepers should enable users to freely choose to consent to the processing of their personal data, by offering a less personalised but equivalent alternative.<sup>17</sup> Recital 37 explains that, in principle, the less personalised alternative should not be different or of degraded quality.<sup>18</sup>

The EDPB notes that it cannot *in abstracto* assess whether the offering of a paid alternative to a service that involves tracking, mentioned in draft principles B-D, would ensure that a valid consent could be obtained for any processing for tracking of users for advertising purposes. When assessing whether consent is valid, the EDPB considers it among others relevant whether in addition to a service using tracking technology and a paid service, another type of service is offered, for example a service with a less privacy intrusive form of advertising, such as contextual advertising, and whether the data subject is able to exercise a real choice.

The European Court of Justice ruled in its judgment of 4 July 2023 that in the specific circumstances it assessed, it must be possible for a user to refuse to give consent without the user being obliged to refrain entirely from using the service. It considered that those users are to be offered, if necessary for an appropriate fee, an equivalent alternative not accompanied by the data processing operations in question.<sup>19</sup> This means that if users decide not to give any consent, only storage and accessing

---

<sup>16</sup> OJ L 265, 12.10.2022, p. 1–66.

<sup>17</sup> Recital 36 Digital Markets Act: “[t]o ensure that gatekeepers do not unfairly undermine the contestability of core platform services, gatekeepers should enable end users to freely choose to opt-in to such data processing and sign-in practices by offering a less personalised but equivalent alternative, and without making the use of the core platform service or certain functionalities thereof conditional upon the end user’s consent.”

<sup>18</sup> Recital 37 Digital Markets Act: “[t]he less personalised alternative should not be different or of degraded quality compared to the service provided to the end users who provide consent, unless a degradation of quality is a direct consequence of the gatekeeper not being able to process such personal data or signing in end users to a service.”

<sup>19</sup> Judgment of 4 July 2023, Meta Platforms and others (General terms of use of a social network), C-252/21, ECLI:EU:C:2023:537, paragraph 150.

processes that are exempted from consent under Article 5(3) ePrivacy Directive may be carried out. The EDPB notes that the aforementioned analysis may differ depending on the circumstances of the case.

Taking into account the above, the EDPB recommends that the draft principles reflect the need for a case by case analysis of whether consent is freely given and valid, taking into account the different options provided to the user.

For the sake of completeness, the EDPB also recalls that cookies may serve multiple functions, beyond the implementation of a business model. The EDPB therefore recommends that the first sentence of draft principle C is amended to indicate that “cookies *may* be used to implement a business model”.

## 4 DRAFT PRINCIPLE E

*E. Consent to cookies for advertising purposes should not be necessary for every single tracker. For those interested, in a second layer, more information on the types of cookies used for advertising purposes should be given, with a possibility to make a more fine-grained selection.*

When users agree to receive advertising, it should be made clear to them at the same time how this is carried out and especially if cookies, including if relevant third-party cookies, are placed on their device. It should not be necessary for them to check every single tracker. Indeed, this may request checking one to two thousand different partners, making the choice totally ineffective and either giving an illusion of choice or discouraging people to read further, leading them to press “accept all” or “refuse all” buttons. This principle should be without prejudice to stricter rules in other sectoral legislation, such as the DMA.

Draft principle E also relates to the requirements of valid consent. The EDPB recalls its Guidelines 05/2020, as also mentioned in its feedback to draft principles B-D. More in particular, the EDPB points out that for consent to be valid, it must be *freely given*,<sup>20</sup> and it must be *specific*.<sup>21</sup>

The EDPB recommends explicitly confirming in the draft principles that individuals should be provided with the opportunity to “reject” all cookies that are not strictly necessary on the first layer of the banner. At a minimum, it should be clarified that if an “accept” (or “accept all”) button is presented on any layer, then a “reject” (or “reject all”) button should also be presented as this would be an essential element in favour of the validity of consent.<sup>22</sup>

Further, as discussed above, for consent to be valid, the user must be informed among others about the identity of the controller that asks for consent to access or store information in terminal equipment, which information it concerns, and for what purpose.<sup>23</sup>

The EDPB agrees that it is possible to consent to cookies for a specific advertising purpose without necessarily requiring users to separately consent to every single tracker or partner on the first layer of a cookie banner, combined with the possibility for the user to make a more granular choice per

---

<sup>20</sup> See also EDPB [Guidelines 05/2020 on consent under Regulation 2016/679](#), adopted on 4 May 2020, section 3.1.

<sup>21</sup> See also EDPB [Guidelines 05/2020 on consent under Regulation 2016/679](#), adopted on 4 May 2020, section 3.2.

<sup>22</sup> See also EDPB [Report of the work undertaken by the Cookie Banner Taskforce](#), adopted on 17 January 2023, Type A Practice – “No Reject Button On The First Layer”.

<sup>23</sup> EDPB [Guidelines 05/2020 on consent under Regulation 2016/679](#), adopted on 4 May 2020, paragraph 64.

controller per specific purpose on the second layer. Compliance with the GDPR requirements for valid consent of such set-up must be assessed taking into account among others Guidelines 05/2020,<sup>24</sup> the Guidelines on transparency under Regulation 2016/679<sup>25</sup> and the Guidelines 03/2022.<sup>26</sup> Further, the specific circumstances of the implementation are relevant. For example, the EDPB considers it unlikely that the use of a very large number of partners for a single purpose would meet the requirements of necessity and proportionality and consent would therefore unlikely be valid. The EDPB, therefore, suggests to clarify that, in any case, consent must be, in particular, informed and unambiguous, and that this may be more difficult to achieve if the number of partners is increasing.

Further, the EDPB suggests specifying that the user, when asked for consent, should be provided with the identity of the actors that actually access/store information in the terminal equipment and/or with whom data is subsequently shared, if applicable, and should not be provided with a list of potential actors.

## 5 DRAFT PRINCIPLE F

*F. No separate consent for cookies used to manage the advertising model selected by the consumer (e.g. cookies to measure performance of a specific ad or to perform contextual advertising) will be required as the consumers have already expressed their choice to one of the business models.*

One reason of the cookie fatigue is that all types of cookies are very often described in a lengthy and rather technical fashion that render an informed choice complex and cumbersome and de facto ineffective. Furthermore, from the moment the business model is made clear and agreed by the consumer, the need of businesses to measure the performance of their advertising services can be deemed inextricably linked to the business model of advertising, to which the consumer has consented. Other cookies not strictly necessary for the delivery of the specific advertising service should still require a separate consent.

As mentioned, according to data protection rules, consent must be requested for a *specific* purpose of the processing. Such purpose must be well defined and precise, in order to determine which processing activities take place for the purpose.<sup>27</sup> Further, for consent to be valid, purposes should not be combined.<sup>28</sup> If a user consents to access or storage of information in their terminal equipment for a well described advertising purpose, such purpose may concern technical processing operations intrinsically linked to the advertising purpose, such as the use of cookies for frequency capping or measuring the effectiveness of ad campaigns. Such technical processing operations may involve access or storage of information in terminal equipment. The users should be informed of such technical

<sup>24</sup> EDPB [Guidelines 05/2020 on consent under Regulation 2016/679](#), adopted on 4 May 2020.

<sup>25</sup> [Article 29 Working Party Guidelines on transparency under Regulation 2016/679](#), adopted on 29 November 2017, last Revised and Adopted on 11 April 2018.

<sup>26</sup> EDPB [Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them](#), adopted on 14 February 2023.

<sup>27</sup> Article 29 Working Party [Opinion 03/2013 on purpose limitation](#), adopted on 2 April 2013, p. 15-16: “The purpose of the collection must be clearly and specifically identified: it must be detailed enough to determine what kind of processing is and is not included within the specified purpose, and to allow that compliance with the law can be assessed and data protection safeguards applied. For these reasons, a purpose that is vague or general, such as for instance ‘improving users’ experience’, ‘marketing purposes’, ‘IT-security purposes’ or ‘future research’ will - without more detail - usually not meet the criteria of being ‘specific’.” See also [Article 29 Working Party Guidelines on transparency under Regulation 2016/679](#), adopted on 29 November 2017, last Revised and Adopted on 11 April 2018, paragraph 12.

<sup>28</sup> Recital 32 GDPR: “When the processing has multiple purposes, consent should be given for all of them.”

processing operations, for example on the second layer of the cookie banner. Conversely, the consent to use of cookies for specific advertising purposes would not extend to other processing operations that are not strictly necessary for that purpose, such as the collection and use of email addresses of a website to send marketing emails.

The EDPB also notes that draft principle F refers to a business model “agreed” by the consumer and a model of advertising to which the consumer has “consented”. Under Article 5(3) ePrivacy Directive, consent is given to access or storage of information (e.g. cookies) in the user’s terminal equipment. The EDPB recognizes that for an advertising business model, cookies may be used, and recommends for the sake of clarity clarifying the explanation to draft principle F, by referring to consent for the use of cookies for a specific model of advertising, as opposed to consent to a model of advertising.

## 6 DRAFT PRINCIPLE G

*G. The consumer should not be asked to accept cookies in one year period of time since the last request. The cookie to record the consumer’s refusal is necessary to respect his/her choice.*

One major reason of the cookie fatigue especially felt by the persons most interested in their privacy is that negative choices are not recorded and need to be repeated each time they visit a website or even every page of a website. Recording such choice is indispensable for an efficient management of a website and for respecting consumers’ choices. Furthermore, to reduce the cookie fatigue, a reasonable period e.g. a year should be adopted before asking again for consumers’ consent.

The EDPB understands that the scope of draft principle G relates only to the recording of a user’s refusal to, or withdrawal of, consent. The EDPB recommends clarifying the first sentence of the draft principle in this respect.

The EDPB agrees that to make the refusal to, or withdrawal of, consent effective, it may be necessary to record the decision of the user for a certain period, in order to reduce the frequency of consent request a user receives. The EDPB believes the proposed period of one year to be adequate for this purpose.

In addition, draft principle G on the recording of “negative consent” requires further details to effectively implement it. In particular, the EDPB recommend clarifying that the record of the “negative consent” relying on cookies should not contain a unique identifier, but should rather contain generic information, a flag or code, which is common to all users who have refused consent. The EDPB recalls that cookies recording the refusal of consent may be deleted by the user, or deleted due to a change of technical settings, within the one-year period. In such event, when the controller does not have access to the record of the consent refusal anymore, the EDPB considers it reasonable to prompt the user with a new consent request.

The EDPB further recalls that gatekeepers subject to the Digital Markets Act are already subject to rules on the frequency of prompting users to give consent, who initially did not consent or who withdrew their consent.<sup>29</sup>

---

<sup>29</sup> Recital 37 Digital Markets Act: “*Gatekeepers should not design, organise or operate their online interfaces in a way that deceives, manipulates or otherwise materially distorts or impairs the ability of end users to freely give consent. In particular, gatekeepers should not be allowed to prompt end users more than once a year to give consent for the same processing purpose in respect of which they initially did not give consent or withdrew their consent.*”

## 7 DRAFT PRINCIPLE H

*H. Signals from applications providing consumers with the possibility to record their cookie preferences in advance with at least the same principles as described above will be accepted.*

Consumers should have their say if they decide that they want to systematically refuse certain types of advertising models. They should be empowered to do this and privacy and data protection legislation should not be used as an argument against such a choice provided the automated choice has been made consciously.

The EDPB recognises the abilities of software applications to empower users to protect their terminal equipment. The EDPB encourages the employment of data protection by default or design in such applications. The EDPB believes that software settings are a useful tool for users and supports the objective of draft principle H to enable users to express their choice to refuse any access or storage of information in terminal equipment via such settings. The EDPB believes that a pledge to respect the signals/settings expressing a user's refusal, and to not still ask users for consent, could help to reduce cookie fatigue.

Conversely, the EDPB considers that caution is necessary when aiming to use software settings to express affirmative consent. For consent to be valid, users must make an active choice (i.e. a default "yes" would not constitute a valid consent), and it must among others be specific and informed, with regards to the specific context in which this consent is given. The EDPB notes that it has not assessed yet any current use of signals from applications or software settings regarding the use of cookies that offer the granularity, specificity and information to ensure that consent can be validly given in advance.

Finally, the EDPB agrees that privacy and data protection legislation should not be used as an argument to not give effect to an individual's preference to systematically refuse certain types of advertising models.

**Anu Talus**

Chair of the European Data Protection Board

Personal Information Protection Commission  
209, Sejong-daero, Jongno-gu  
Seoul, 03171  
Republic of Korea

Brussels, 20 June 2023

*by e-mail only*

Ref: OUT2023-0044

Dear Mr. Ko,

Thank you very much for your letter of 16 May 2023, addressed to Andrea Jelinek as Chair of the EDPB, to which I am replying after being elected as new Chair of the EDPB on 25 May 2023.

I take note of your two questions linked to recent decisions of the Personal Information Protection Commission.

As a preliminary remark, I must underline that it goes beyond the EDPB's remit to provide any kind of legal advice and/or opinion with regard to individual cases or the practices of individual controllers in non-EU countries. Within its mission of ensuring the consistent application of the GDPR, the EDPB has however issued guidance that can be relevant to your questions, bearing in mind that they refer specifically to the interpretation and application of the GDPR itself.

In your first question you request the EDPB's views as to which party (i.e. the website operator, or the plugin provider) is obliged to obtain consent under the GDPR regarding the collection of users' online behavioural data using cookies and online identifiers.

In this context, you refer to the Judgement of the Court of Justice of the European Union (CJEU) regarding Fashion ID vs Verbraucherzentrale NRW e.V.<sup>1</sup> In this ruling, the CJEU concluded that a website operator which embeds a social media plugin on its website causing the browser of a visitor to that website to request content from the provider of that plugin and, to that end, to transmit to that provider personal data of the visitor, can be considered a controller, jointly with the social media

---

<sup>1</sup> Fashion ID GmbH & Co. KG va Verbraucherzentrale NRW e.V. (Case C-40/17), ECLI:EU:C:2019:629 (hereafter: Case C-40/17)

plugin provider, in respect of operations for which it determines the purposes and means of the processing, i.e. the collection and disclosure by transmission of the personal data of that visitor.<sup>2</sup> The CJEU further stated that consent must be given prior to the collection and disclosure by transmission of the data subject's data to the social media plugin provider<sup>3</sup>. In such circumstances, it is for the operator of the website, rather than for the provider of the social plugin, to obtain that consent, since it is the fact that the visitor consults that website that triggers the processing of the personal data in that case<sup>4</sup>. However, the consent that must be given to the operator relates only to the operation or set of operations involving the processing of personal data in respect of which the operator actually determines the purposes and means.<sup>5</sup>

A first important point to be borne in mind is that the judgment of the CJEU in *Fashion ID* is anchored in the concept of joint controllership, which refers to the situation where two or more entities jointly determine the purposes and means of processing<sup>6</sup>. The EDPB has issued guidance on the concept of (joint) controllership in its Guidelines 7/2020 on the concepts of controller and processor, clarifying that the qualification as controller has to be assessed with regard to each specific data processing activity<sup>7</sup>. With reference, specifically, to joint controllership and the element of jointly determining the means of processing, the EDPB clarified that joint controllers can be such when they process the data for the same purposes but also when they pursue purposes which are closely linked or complementary, e.g. when a mutual benefit arises from the same processing operation and each of the entities involved participates in the determination of the purposes and means of processing.<sup>8</sup> With respect to the joint controllers' decision on the means for processing, the EDPB built upon the judgment in *Fashion ID* to note that "the choice made by an entity to use for its own purposes a tool or other system developed by another entity, allowing the processing of personal data, will likely amount to a joint decision on the means of that processing by those entities"<sup>9</sup>, but clarified that "the use of a common data processing system or infrastructure will not in all cases lead to qualify the parties involved as joint controllers"<sup>10</sup>.

Additionally, in its Guidelines 8/2020 on the targeting of social media users, which you have referenced in your letter, the EDPB has underlined that, where (joint) controllers seek to rely on consent, valid consent must be obtained prior to the processing, and that it is the responsibility of the (joint) controllers to assess when and how information on the processing of personal data should be provided, and consent obtained. The question of which joint controller is in charge of collecting this

---

<sup>2</sup> Case C-40/17, paragraphs 99-101.

<sup>3</sup> Case C-40/17, paragraph 102.

<sup>4</sup> Case C-40/17, paragraph 102.

<sup>5</sup> Case C-40/17, paragraph 102.

<sup>6</sup> Regulation 2016/679 (hereafter: GDPR), Article 4(7) and Article 26.

<sup>7</sup> EDPB Guidelines 7/2020 on the concepts of controller and processor, paragraph 26.

<sup>8</sup> EDPB Guidelines 7/2020 on the concepts of controller and processor, paragraph 59-60.

<sup>9</sup> EDPB Guidelines 7/2020 on the concepts of controller and processor, paragraph 67. The EDPB also noted that the CJEU concluded "that by embedding on its website the Facebook Like button made available by Facebook to website operators, *Fashion ID* has exerted a decisive influence in respect of the operations involving the collection and transmission of the personal data of the visitors of its website to Facebook and had thus jointly determined with Facebook the means of that processing" (referring to Case 40/17, paragraphs 77-79).

<sup>10</sup> EDPB Guidelines 7/2020 on the concepts of controller and processor, paragraph 68.

consent comes down to determining which of them is involved first with the data subject.<sup>11</sup> In practice, therefore, the EDPB's view is that this question will depend on the circumstances of the specific case at hand.

As to example 6 of these guidelines, as the placement of cookies and processing of personal data occurred at the moment of account creation, the EDPB considers that the social media provider had to collect her valid consent before the placement of advertisement cookies<sup>12</sup>. However, another point that was highlighted by the EDPB is that where consent is relied upon by multiple (joint) controllers or if the data is to be transferred to or processed by other controllers who wish to rely on the original consent, these organisations should all be named, and insofar as not all joint controllers are known at the moment when the social media provider seeks the consent, the latter will necessarily need to be complemented by further information and consent collected by the website operator embedding the social media plugin<sup>13</sup>. This was illustrated in example 6 of the Guidelines, where the website operator sought consent to transmit the personal data to the social media provider and undertook technical measures so that no personal data is transferred to the social media platform until she gives her consent.<sup>14</sup>

It is also to be emphasised that the consent that may have to be collected by the website operator relates only to the operation or set of operations involving the processing of personal data in respect of which the operator actually determines the purposes and means<sup>15</sup>. Consequently, the EDPB underlined that the collection of consent by a website operator does not negate or in any way diminish the obligation of the social media provider to ensure the data subject has provided a valid consent for the processing for which it is responsible, either as a joint controller or as a sole controller.

As regards your second request to provide EDPB's views on the data processing practices of large technology companies and claims that are made by these companies, including concerns over potential data protection and privacy infringements, as mentioned above, the EDPB cannot provide legal advice on specific cases outside of its remit, nor make general statements about any category of controllers and their practices in third countries.

As regards the three national decisions you have referenced, I would like to underline that as all national decisions, these were taken based on the circumstances of those specific cases, and do not cover the practices of controllers in third countries' jurisdictions.

---

<sup>11</sup> EDPB Guidelines 8/2020 on the targeting of social media users, paragraph 74.

<sup>12</sup> EDPB Guidelines 8/2020 on the targeting of social media users, paragraph 74.

<sup>13</sup> EDPB Guidelines 8/2020 on the targeting of social media users, paragraph 75; EDPB Guidelines 5/2020 on consent under Regulation 2016/679, paragraph 65. According to the EDPB, insofar as not all joint controllers are known at the moment when the social media provider seeks the consent, the latter will necessarily need to be complemented by further information and consent collected by the website operator embedding the social media plugin. EDPB Guidelines 8/2020 on the targeting of social media users, paragraph 75.

<sup>14</sup> EDPB Guidelines 8/2020 on the targeting of social media users, paragraph 74, and example 6 on p. 21.

<sup>15</sup> EDPB Guidelines 8/2020 on the targeting of social media users, paragraph 76, referring to Case 40/17 paragraphs 100-101.



European Data Protection Board

I trust that these explanations and the documents we refer to may be helpful and clarify the work carried out by the EDPB with a view of ensuring a consistent application of the GDPR in respect of the issues mentioned in your letter.

Yours sincerely

Anu Talus



European Data Protection Board

**Anu Talus**  
Chair of the European Data Protection Board

John Edwards  
Wycliffe House  
Water Lane  
Wilmslow  
Cheshire  
SK9 5AF  
United Kingdom

Brussels, 16/04/2024

EDPB Ref: OUT2024-0040  
ICO Ref: ICO/O/JE/L/MIS/0675

***Subject: Data Protection and Digital Information Bill - EDPB reply letter***

Dear Mr Edwards

Thank you for your letter of 1 March 2024 sharing information on the passage of the Data Protection and Digital Information Bill ("the bill") as it enters the latter stages of consideration by the UK Parliament.

The European Commission is responsible for negotiating and monitoring adequacy decisions. The EDPB has been closely following the developments in the UK and receives regular updates from the European Commission.

Should the European Commission decide to renew the UK adequacy decisions before the end of the sunset clause expiry date, then it should consult the EDPB for an Opinion in accordance with Article 70(1)(s) GDPR. The EDPB is looking forward to contributing to the European Commission's evaluation of the UK adequacy decisions.

Yours sincerely,

Anu Talus

European Data Protection Board  
Rue Wiertz, 60  
1047 Brussels

**Anu Talus**  
Chair of the European Data Protection Board

Mr. Miguel de Serpa Soares  
Under-Secretary-General for Legal Affairs and United Nations Legal Counsel United Nations N.Y. 10017  
United States

Brussels, 23 May 2024

Ref: OUT2024-0047

Dear Mr. Serpa Soares,

Thank you for your kind words on my election as new Chair of the European Data Protection Board (“the Board” or the “EDPB”) and for your letter of 6 February 2024, by which you refer to the ongoing dialogue between the EDPB and the United Nations System Organisations on data protection related matters. This letter is a follow-up to your previous letters of 26 February 2020, 14 May 2020, and of 15 July 2021, on a similar subject-matter to which the former EDPB Chair replied on 7 October 2020<sup>1</sup> and on 18 November 2021<sup>2</sup>.

As part of the international community, both the United Nations and the European Union ('EU') are grounded in the principle of the rule of law and a commitment to uphold human rights and values which are enshrined in their foundational treaties and which determine their operational frameworks.

Within the EU framework, the Board and its members need to ensure that entities that are subject to EU law respect and adhere to the fundamental right of protection of personal data, including as reflected in secondary legislation. Entities that transfer personal data to entities in third countries or international organisations ('IOs') need to comply with EU data protection law, including their rules on international transfers under Chapter V of Regulation 2016/679 and Chapter V of Regulation (EU) 2018/1725.

In that respect, the Board expresses its gratitude for the valuable comments you have submitted concerning the 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<sup>3</sup>. The Board is of the opinion that this document as well as additional guidance<sup>4</sup> already provide clarifications having regard to transfers to IOs, which are also relevant for United Nations System Organisations. This for

<sup>1</sup> [https://www.edpb.europa.eu/sites/default/files/files/file1/edpb\\_letter\\_out2020-0109\\_un.pdf](https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_letter_out2020-0109_un.pdf)

<sup>2</sup> [https://www.edpb.europa.eu/system/files/2021-11/edpb\\_letter\\_out2021-00156\\_un\\_en.pdf](https://www.edpb.europa.eu/system/files/2021-11/edpb_letter_out2021-00156_un_en.pdf)

<sup>3</sup> [https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22020-articles-46-2-and-46-3-b-regulation\\_en](https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22020-articles-46-2-and-46-3-b-regulation_en)

<sup>4</sup> See in particular Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, as adopted by the European Data Protection Board on 25 May 2018 ; or the Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)



European Data Protection Board

instance includes clarifications on privileges and immunities under international law as well as developing safeguards that take into account the status and features of IOs (e.g. recognising that independent oversight and redress can be ensured by other bodies than national data protection authorities and courts).

With regard to the references made in your letter on initiatives undertaken by the European Data Protection Supervisor (EDPS) under Regulation (EU) 2018/1725 and by the European Commission (EC), the Board notes that it is not the role of the EDPB to reply on behalf of these two institutions. Having mentioned this, the Board welcomes the active participation of representatives of many IOs, including the UN System Organisations, in the Task Force on transfers to international organisations established by the EDPS (the 'Task Force'), which involves also national data protection authorities and the EC.

The Board observes that the work of the Task Force is useful to allow its participants to share views on different aspects relating to data transfers to international organisations and explore practical solutions to enable controllers and processors that are based in the EEA to transfer personal data to IOs that are compliant with the EU data protection laws. The Board takes note that the Task Force's focus on practical transfer tools and solutions is the result of the preferences expressed by a large majority of participants in the Task Force.

It is worth mentioning that the participation in these discussions is not considered an acceptance or endorsement of specific documents or instruments by the Task Force, as the Task Force is meant to be an informal forum for discussions among stakeholders and to collect input from international organisations. This input has for instance contributed to the development by the EDPS of a model administrative arrangement for transfers of personal data under Regulation (EU) 2018/1725 from EU Institutions, bodies, offices and agencies to international organisations. The Board encourages the representatives of the United Nations Organisations to keep constructively participating in this Task Force.

In your letter you refer to a specific document which is a first working draft of possible model contractual clauses that has been shared by the EC on a purely informal basis with representatives of IOs in the framework of the Taskforce. I understand that this work has been initiated – and the informal consultation has been conducted – at the request of IOs with a view to address, through a practical instrument, a concrete scenario which many IOs are confronted with, namely transfers of personal data from Processors in the EU to IOs. The aim of the consultations is to explore the possibility of developing standard contractual clauses specifically covering the aforementioned scenario and to facilitate compliance by EU processors with their obligations under EU data protection law, while duly taking into account the status, nature and legal framework applicable to IOs. To the knowledge of the Board, the document which you refer to is still under development and could offer an additional available compliance tool if the work is successfully concluded. The Board recalls that there would be no obligation for IOs to use such clauses. I understand that several organisations have expressed an interest in continuing this work.



European Data Protection Board

As recalled prior, the EDPB members have published useful guidance that covers, among others, aspects of transfers to IOs, which is also relevant to the United Nations System Organisations. The Task Force established by the EDPS is developing practical tools that support this guidance. The Board and its members support these endeavours and welcome the participation of the United Nations System Organisations in this forum. As indicated by my predecessor in her previous letters, the work carried out in this Task Force cannot, in any way, replace formal procedures set out in the GDPR.

Lastly, I would like to renew the Board's commitment to engage further with the United Nations System Organisations on the shared mission to protect human rights including the right to privacy.

Yours sincerely

Anu Talus

European Data Protection Board  
Rue Wiertz, 60  
1047 Brussels

**Anu Talus**  
Chair of the European Data Protection Board

Rita Wezenbeek  
Director CNECT.F  
DG for  
Communications Networks, Content and Technology  
European Commission  
1049 Brussels  
Belgium

Alberto Bacchiesa  
Director COMP.J  
DG General for Competition  
European Commission  
Place Madou 1  
1210 Brussels  
Belgium

Brussels, 30 May 2024

*by e-mail only*

EDPB Ref: OUT2024-048

**Subject: Article 15 DMA Consumer Profiling Reports**

Dear Ms. Rita Wezenbeek, Dear Mr. Alberto Bacchiesa,

Thank you for your letter of 22 March 2024 and for transmitting the six Consumer Profiling Reports (“the reports”) submitted by gatekeepers pursuant to Article 15 of the Digital Markets Act (“DMA”). The EDPB takes note that these reports are of a confidential nature and confirms that they will be treated as such.

The EDPB is currently analysing the reports with a view of assessing the possible use of for purposes of Regulation 2016/679 (“GDPR”), and in particular to inform the enforcement of Union data protection rules, as provided for by Article 36(3) and recital 72 DMA.

The EDPB also takes note of the Commission’s invitation for the EDPB to provide its views on the content of the reports and takes note that the Commission would consider having a dedicated discussion on these reports during one of the next meetings of the DMA High Level Group (HLG).

Cooperation with other regulatory authorities on matters with an impact on data protection is of great importance to the EDPB, and is a key pillar in the EDPB Strategy 2024-2027. The EDPB and its members look forward to continue cooperation with the Commission in the context of the DMA and to contribute to the work of the DMA HLG.

Yours sincerely,

Anu Talus

Ms Sophie in 't Veld,  
Mr Moritz Körner,  
Mr Michal Šimečka,  
Ms Fabiene Keller,  
Mr Jan-Christoph Oetjen,  
Ms Anna Donáth,  
Ms Maite Pagazaurtundúa,  
Mr Olivier Chastel,  
Members of the European Parliament

10 June 2020

By email only

Ref: OUT2020-0052

Dear Members of the European Parliament,

Thank you for your letter concerning the facial recognition app developed by Clearview AI and for your continued vigilance in protecting the personal data of individuals in the Union. The EDPB naturally shares your commitment and is, beyond this case, particularly concerned by certain developments in the European Union and around the world regarding facial recognition technologies, which raise unprecedented issues from the point of view of data protection.

Facial recognition technology may undermine the right to respect for private life and the protection of personal data, but also other fundamental rights and freedoms (in particular freedom of expression and information, freedom of assembly and association, and freedom of thought, conscience and religion). It may also affect individuals' reasonable expectation of anonymity in public spaces. Such technology also raises wider issues from an ethical and societal point of view.

Regarding the service offered by Clearview AI, the EDPB is aware of media reports indicating that the company has been in contact with national law enforcement agencies, government bodies, and police forces in several EU Member States. The EDPB furthermore has taken note of the public acknowledgement of limited use by police forces in one of the Member States. The EDPB also notes that since Clearview AI's database is allegedly set up by "scraping" photographs and facial pictures accessible online, in particular those made available via social networks, the possible use of this service by law enforcement authorities (comparing photos through facial recognition analysis against the database) is likely to entail the processing of biometric data of persons in the European Union.

Based on the information at its disposal to date, the EDPB is in a position to share some preliminary answers to the questions you raised. This preliminary assessment focuses on the compliance and lawfulness of processing resulting from the possible use by EU law enforcement authorities of a service such as offered by Clearview AI. For your information, several EDPB members have already started to further inquire about the use of such facial recognition technologies in their respective jurisdictions. Please note that for the investigation and enforcement of individual cases the competency lies with each individual member of the EDPB.

## *On the possible use of the Clearview AI application by law enforcement authorities in the EU*

The EDPB notes that under the Law Enforcement Directive (EU) 2016/680, law enforcement authorities in the Union may process biometric data for the purpose of uniquely identifying a natural person only in accordance with the strict conditions of Articles 8 and 10 of the Directive. According to Article 8, such processing can only take place to the extent necessary for the performance of a task for purposes to which the Directive applies and that is based on Union or Member State law, which must comply with the EU Charter of Fundamental Rights as well as the European Convention on Human Rights. In addition, Art. 10 requires such processing, *inter alia*, to be strictly necessary and subject to appropriate safeguards for the rights and freedoms of data subjects.<sup>1</sup> In line with these strict conditions, EU law enforcement authorities may under certain circumstances process certain biometric data, including biometric templates from photos and check these against biometric templates in databases that are under the control of the official authorities and that have been established under Union or Member State law.

The possible use of a service such as offered by Clearview AI by law enforcement authorities would, however, be fundamentally different, in that it would imply, as part of a police or criminal investigation, the sharing of personal data with a private party outside the Union and the biometric matching of such data against the latter's mass and arbitrarily populated database of photographs and facial pictures accessible online.

The EDPB has doubts as to whether any Union or Member State law provides a legal basis for using a service such as offered by Clearview AI. Therefore, as it stands and without prejudice to any future or pending investigation, the lawfulness of such use by EU law enforcement authorities cannot be ascertained.

In addition, the EDPB considers that processing of personal data in a law enforcement context that would rely on a database populated by collection of personal data on a mass-scale and in an indiscriminate way without any limitation, or any precise connection between the data collected and the objective pursued would, as such, likely not meet the strict necessity requirement provided for by the Directive. As regards observance of this principle of proportionality, the protection of the fundamental right to respect for private life at EU level requires, in accordance with settled case-law of the Court of Justice of the European Union, that derogations from and limitations to the protection of personal data should apply only in so far as it is strictly necessary.<sup>2</sup>

---

<sup>1</sup> The need for safeguards is all the greater where personal data is subject to automated processing. Those considerations apply particularly where the protection of the particular category of personal data that is sensitive data is at stake (see, to that effect, judgments of 8 April 2014, Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 54 and 55, and of 21 December 2016, Tele2 Sverige and Watson and Others, C-203/15 and C-698/15, EU:C:2016:970, paragraphs 109 and 117; see, to that effect, ECtHR, 4 December 2008, S. and Marper v. the United Kingdom, CE:ECHR:2008:1204JUD003056204, § 103).

<sup>2</sup> (judgments of 16 December 2008, Satakunnan Markkinapörssi and Satamedia, C-73/07, EU:C:2008:727, paragraph 56; of 8 April 2014, Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 51 and 52; of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, paragraph 92; and of 21 December 2016, Tele2 Sverige and Watson and Others, C-203/15 and C-698/15, EU:C:2016:970, paragraphs 96 and 103).

**Andrea Jelinek**

Chair of the European Data Protection Board

rue Wiertz, 60  
1047 Brussels

Finally, the EDPB notes that the possible use by EU law enforcement authorities of an application made available by a data controller with established operations outside the Union such as Clearview AI would constitute a transfer of personal data from the Union to the United States of America, where the company is established (e.g. the transfer of personal data of those whose identity is sought through the use of the facial recognition service). The EDPB notes in particular that the transfer of personal data would not be subject to the provisions of the EU-US Privacy Shield adequacy decision, nor to the EU-US Umbrella Agreement. To be lawful, such a transfer would have to be compliant with the strict conditions and requirements set in Article 39 of the Law Enforcement Directive that governs specifically transfers from EU law enforcement authorities to private operators in third countries.

Without prejudice to further analysis on the basis of additional elements provided, the EDPB is therefore of the opinion that the use of a service such as Clearview AI by law enforcement authorities in the European Union would, as it stands, likely not be consistent with the EU data protection regime.

#### *On the possible use of the Clearview AI application by intelligence services in the EU*

In view of its competence, the EDPB this letter focuses primarily on the possible use of an application such as the Clearview AI by law enforcement authorities.

While questions relating to processing in the area of national security fall only partly within the scope of EU law and therefore the competence of the EDPB, it should be recalled that at any rate, processing of this data by intelligence services should, always, be carried out under conditions complying with the provisions of the European Convention on Human Rights, as interpreted by the European Court of Human Rights, and Convention 108.

#### *On the EDPB initiatives related to facial recognition technologies*

This preliminary assessment by the EDPB is without prejudice to any initiative or formal decisions that national supervisory authorities may wish to take in respect of both the processing carried out by Clearview AI on its own behalf under the GDPR and the possible use of such service by law enforcement agencies, as well as intelligence authorities when falling within the scope of their competence, in the EU.

The EDPB is committed to continuing its work on analysing the use of facial recognition in its various forms. The EDPB guidelines adopted in January 2020 on processing of personal data through video devices already address this technology and several supervisory authorities have also taken positions or adopted decisions on specific cases involving facial recognition. This work will be continued by the EDPB, in particular with a view to inform future legislative work at European and national level, also with regard to the use of facial recognition technology by law enforcement authorities.

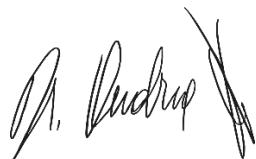
The EDPB considers that, beyond the need for compliance with the EU data protection *acquis*, facial recognition - for which different usages raise different issues - calls for political choices to be made:

**Andrea Jelinek**  
Chair of the European Data Protection Board

rue Wiertz, 60  
1047 Brussels

as to the role a democratic society is ready to give this technology and how it affects the fundamental rights and freedoms of individuals. The EDPB is willing to contribute, within the limits of its competence, to the necessary political decision-making on this matter. In this context, the EDPB considers that the recent White Paper of the European Commission on artificial intelligence provides an opportunity for such debate which should lead to the determination of cases in which facial recognition is acceptable and necessary in a democratic society and cases in which it is not.

Yours sincerely,



Andrea Jelinek

15 June 2020

By email only

Ref: OUT 2020-0054

Dear Members of the European Parliament,

I would like to thank you for your letter dated 10<sup>th</sup> January 2020 regarding the agreement between the UK and the US on Access to Electronic Data for the Purpose of Countering Serious Crime<sup>1</sup>, signed on 3<sup>rd</sup> October 2019.

As a preamble to its answer, the EDPB would like to stress that it can at this stage only provide a preliminary analysis, on the basis of the elements at its disposal, and that the date of effective application of this agreement is likely to impact on any legal assessment and conclusion, given the applicable transitional period for the withdrawal of the UK from the European Union. Indeed, as per the Brexit withdrawal agreement, EU law continues to apply until the end of the transitional period, currently set for 31<sup>st</sup> December 2020, while this should no longer be the case as of 1<sup>st</sup> January 2021.

The EDPB first recalls that the European Commission and, ultimately, the Court of Justice of the European Union are the EU Institutions competent to assess whether, as per the Treaties and EU secondary law, the United Kingdom was in a capacity to enter into an agreement with the United States regulating access to personal data between both countries for the purpose of preventing and prosecuting serious crime. With regard to the compatibility of the agreement at stake with the EU *acquis* in the field of data protection, and in particular with the GDPR and the law enforcement directive, the EDPB stresses that the level of personal data protection, including substantive and procedural conditions for access to personal data, needs to be ensured consistently throughout the Union.

Considering the provisions of the agreement, read in conjunction with Sections 3 of the US CLOUD Act<sup>2</sup>, the EDPB has doubts as to whether the safeguards in the agreement for access to personal data in the UK would apply in case of disclosure obligations applicable to providers of electronic communication service or remote computing service under the jurisdiction of the United States, regardless of whether the data requested is located within or outside of the United States. Following this preliminary assessment, it is unclear whether the safeguards enshrined in the Agreement would apply to all, if any, requests for access made under the US CLOUD Act.

---

<sup>1</sup>[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/836969/CS\\_USA\\_6.2019\\_Agreement\\_between\\_the\\_United\\_Kingdom\\_and\\_the\\_USA\\_on\\_Access\\_to\\_Electronic\\_Data\\_for\\_the\\_Purpose\\_of\\_Countering\\_Serious\\_Crime.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf)

<sup>2</sup><https://www.congress.gov/bill/115th-congress/senate-bill/2383/text>

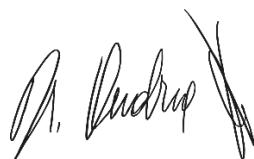
In this regard, as the Commission has entered into negotiations for the conclusion of an EU-US agreement to facilitate access to electronic evidence in criminal investigations, the EDPB stresses that any future agreement between the EU and the US must prevail over US domestic laws and include appropriate data protection safeguards in order to be fully compatible with EU primary and secondary law. This notably includes ensuring the continuity of data protection in case of onward sharing and onward transfers. In this context, the EDPB wishes to repeat its call for further improvements to the level of safeguards established by the EU-US Umbrella Agreement, for instance as regards the availability of judicial redress.

It is also essential that the safeguards include a mandatory prior judicial authorisation as an essential guarantee for access to metadata and content data. On the basis of its preliminary assessment, the EDPB, while noting that the agreement refers to the application of domestic law, could not identify such a clear provision in the agreement concluded between the UK and the US.

Finally, when it comes to a possible adequacy decision for the UK, the EDPB considers that the agreement concluded between the UK and the US will have to be taken into account by the European Commission in its overall assessment of the level of protection of personal data in the UK, in particular as regards the requirement to ensure continuity of protection in case of “onward transfers” from the UK to another third country.

Should the European Commission present a draft adequacy decision for the UK, the EDPB will provide its own assessment in a dedicated opinion.

Yours sincerely,



Andrea Jelinek

Ms. Sophie in 't Veld,  
Mr. Olivier Chastel,  
Mr. Moritz Körner,  
Ms. Maite Pagazaurtundúa,  
Mr. Michal Šimečka,  
Ms. Ramona Strugariu,  
Members of the European Parliament

By email only

28 July 2020

Ref: OUT2020-0090

Dear Members of the European Parliament,

I would like to thank you on behalf of the European Data Protection Board (EDPB) for your questions relating to the possible expansion of the so called Prüm framework.

The EDPB took note of the media reports in this regard but has not been consulted, formally or informally, by the Council or the Commission on this matter. As there is no formal proposal presented to date, I am only in a position to share with you some preliminary elements of our analysis based on and limited to the information publicly available. The EDPB stands ready to provide further in-depth guidance, should a legislative proposal be envisioned.

It has to be stressed that the EU data protection framework has evolved significantly since the 2005 Prüm Treaty and its partial inclusion into the EU acquis with the so-called Prüm Council Decision (2008/615/JHA) and the so-called Swedish Initiative (2006/960/JHA). It is therefore essential that the Prüm framework undergoes a comprehensive and independent evaluation with regard to its compliance with the current data protection acquis, prior to any envisioned expansion or amendment. The EDPB remains available to advise the Commission in this regard. In that respect, the EDPB takes note of the Commission's intention (COM(2020) 262 final, 24.6.2020) to provide for the necessary alignment with the Law Enforcement Directive (Directive 2016/680) when it proposes a revised and modernized Prüm legal framework in 2021.

Whether the Prüm legal framework may be expanded to include retrospective facial recognition (i.e. not live facial recognition), in line with EU law, would also depend on the details of the possible expansion and data protection safeguards foreseen.

The addition of retrospective facial recognition for the purpose of identifying a person within the Prüm legal framework would require a dedicated legal basis under EU law. Furthermore, whether the Prüm legal framework may be expanded to include retrospective facial recognition must first be assessed through a thorough impact assessment, in order to ensure that the necessity and proportionality of such measure, and the essence of the fundamental right to data protection are respected.

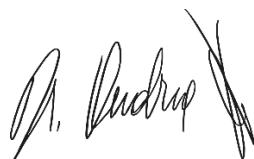
The EDPB indeed sees a great risk that Member States could disproportionately collect and process vast amount of facial recognition data, as the difference between DNA and fingerprint data on the one hand and facial recognition data on the other is, inter alia, that the latter data can be collected much more easily and also without the knowledge of the data subjects.

Concerning your question regarding the scope of the mandate of Europol and the cooperation with third countries, should an amendment in this regard be considered, the EDPB will of course take into account the views of the EDPS (as the supervisory authority of Europol) and the Europol Cooperation Board in order to assess whether the involvement of Europol would be in line with its mandate and EU law.

The EDPB furthermore considers any expansion of the Prüm legal framework with regard to the cooperation with third countries to require particular scrutiny. Transfers to third countries would have to be made strictly on the basis of legally binding instruments including appropriate guarantees, as provided for in the Chapter V LED.

Finally, I would also like to recall that the EDPB will prepare guidelines on the use of facial recognition technology by law enforcement authorities.

Yours sincerely,



Andrea Jelinek

István Ujhelyi  
MEP European Parliament  
Rue Wiertz 60  
B-1047 Brussels  
Belgium

Brussels, 14 December 2021

*By e-mail only*

Ref: OUT2021-00160

Dear Mr Ujhelyi,

Thank you for your letter related to the alleged use of spyware by public authorities in Hungary, in which you draw the European Data Protection Board's (EDPB) attention to specific aspects related to the right to the protection of personal data.

First of all, I would like to underline that the EDPB and its members pay particular attention to the current developments related to the interferences with the fundamental rights to privacy and data protection through surveillance measures, notably following the Pegasus media revelations and its implications in several Member States.

The EDPB is competent in the matter of the alleged use of the Pegasus software mainly if and as far as it is deployed for purposes under the GDPR and the LED.

I would like to also underline that according to the applicable Union law the European Data Protection Board (EDPB) does not have the same competences, tasks and powers as national supervisory authorities. Indeed, at national level, the assessment of alleged infringements of the GDPR, or of the EU overall data protection framework, falls within the competence of the responsible and independent national supervisory authority and, when it comes to matters falling under Union law, subject to the cooperation and consistency mechanisms set out in the GDPR and the LED. Within these mechanisms, one of the EDPB's tasks is the promotion of cooperation and effective bilateral and multilateral exchange of information between the supervisory authorities.<sup>1</sup>

In light of the most recent CJEU case law, the EDPB recalls in this context that access, retention and further use of personal data by public authorities within the remit of surveillance measures must not exceed the limits of what is strictly necessary, assessed in the light of the Charter, otherwise it "cannot be considered to be justified, within a democratic society".<sup>2</sup>

Furthermore, the EDPB already had the occasion to make clear that the protection of journalists and their sources is a cornerstone of the freedom of the press.

---

<sup>1</sup> Article 70(1)(u) GDPR, Article 51(1)(h) LED.

<sup>2</sup> CJEU, Case C-623/17, Privacy International, §81

In relation to the matter raised in your letter, I would like to refer to the official statement of the Hungarian data protection supervisory authority (SA), published on 5 August 2021 regarding its measures to address the issue.<sup>3</sup>

This statement informs that, in accordance with its competences and with the Act CXII of 2011 on the right to informational self-determination and on the freedom of information (Privacy Act) Art. 51/A section (1), the Hungarian SA initiated an ex officio procedure in this case. Until the end of this investigation, and in line with the applicable procedure, the Hungarian SA is not able to share any information with the public on this topic.

Concerning the particular case at stake, the Hungarian National Authority for Data Protection and Freedom of Information, as national supervisory authority, has competency to carry out the investigation procedure regarding the alleged use of spyware by Hungarian authorities. In line with the applicable legal framework, the Hungarian SA has indeed powers to investigate matters related to secret surveillance and processing of classified information.

To conclude, I wish to reassure you that the EDPB will continue to pay special attention to the developments of personal data processing related to surveillance measures in Member States and will remain ready to support all members of the EDPB, including the Hungarian supervisory authority, in such matters.

Yours sincerely,



Andrea Jelinek

---

<sup>3</sup> "An international investigation has revealed that a spyware so called Pegasus developed by Israeli NSO has been installed into the phones of certain target persons." Available: <https://www.naih.hu/tajekoztatok-kozlemenyek>

# Letters



Sophie in't Veld  
MEP European Parliament  
Rue Wiertz 60  
B-1047 Brussels  
Belgium

Brussels, 10 August 2021

*by e-mail only*

Ref: OUT2021-00130

Dear Ms in 't Veld,

Thank you for your letter concerning the use of Automatic Image Recognition System on migrants in Italy. The EDPB dedicates special attention to the issue of facial recognition technologies, which raises unprecedented issues and concerns in terms of data protection.

Whilst facial recognition technologies may generally undermine the right to respect for private life and the protection of personal data, but also other fundamental rights and freedoms (in particular freedom of expression and information, freedom of assembly and association, and freedom of thought, conscience and religion), it clearly engenders wider issues from an ethical and societal point of view, especially when dealing with vulnerable people such as migrants.

Concerning the use of facial recognition technologies to monitor disembarkation operations in Italy by police authorities, the Italian Data Protection Authority, according to the information shared, examined the so called "Sari Real Time System", on the basis of a data protection impact assessment carried out by the Ministry of Interior, in accordance with the national legislation implementing the Law Enforcement Directive (EU) 2016/680<sup>1</sup>, prior to the activation of the said system. In particular, this system was not designed to be used specifically for migration, asylum and border control activities, but in general to operate in support of investigative activities.

---

<sup>1</sup> See Article 23 of the Legislative Decree No 51 of 18 May 2018.

In the negative Opinion issued on 25 March 2021<sup>2</sup>, the Italian DPA, in line with the guidance of the Council of Europe, considered the use of facial recognition technologies to be extremely delicate for the purposes of prevention and prosecution of criminal offence. In particular, the Sari Real Time System would entail an automated processing of biometric data on a large-scale basis, that could also concern people not sought by the police, for instance, persons attending a political demonstration. Even though the impact assessment submitted by the Ministry explained that the images would be deleted immediately, the identification of a person would be achieved through the processing of biometric data of all people present in the monitored space, so as to generate templates comparable with those included in a "watch-list". This would result in a transition of surveillance activities, from targeted surveillance of some individuals to universal surveillance.

Regarding this specific case mentioned in your letter, I would like to stress again that while, for the investigation of the use of the said technologies and the enforcement of the GDPR in individual cases, the competency lies with each national supervisory authority, the role of the EDPB is to ensure the consistent application of the GDPR according to Article 70 of the GDPR and to Article 51 of the LED.

To this end, the EDPB is committed to continuing its work on analysing the use of facial recognition. The EDPB guidelines adopted in January 2020 on processing of personal data through video devices, already address these technologies, and several supervisory authorities have also taken positions or adopted decisions on specific cases involving facial recognition. This is also the case of the Italian SA, as you pointed out in your letter. This work is still ongoing, in particular with a view to steer the future legislative work at European and national levels, especially with regard to the use of facial recognition technologies by law enforcement authorities.

In this regard, it is worth mentioning the Joint Opinion 5/2021 recently adopted by the EDPB and the EDPS on the Commission's proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)<sup>3</sup>, which includes specific restrictions on the use of AI systems for 'real-time' remote biometric identification for the purpose of law enforcement. In this Joint Opinion, the EDPB and the EDPS underlined that the use of AI in the area of police and law enforcement requires

---

<sup>2</sup> See Decision No 127 of 25 March 2021 available at <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9575877>.

<sup>3</sup> See 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) available at [https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal\\_en](https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en)

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.

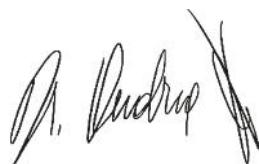
More specifically, they called for a general ban on any use of AI for an automated recognition of human features, such as faces, in publicly accessible spaces, in any context. A ban was equally recommended on AI systems categorising individuals from biometrics, including face recognition, into clusters according to ethnicity or other grounds for discrimination under Article 21 of the Charter. Furthermore, the EDPB and the EDPS considered that the use of AI systems intended to be used by competent public authorities, such as polygraphs and similar tools to detect the emotional state of a natural person, is highly undesirable and should be prohibited.

In addition, as mentioned in its two-year work programme for 2021-2022, the EDPB is currently working on Guidelines on the use of facial recognition technologies in the area of law enforcement.

Therefore, the EDPB is fully aware of the importance of ensuring that the fundamental rights and freedoms of individuals, including the right to privacy and data protection, are adequately safeguarded when individuals' biometric data are subject to automatic processing through facial recognition technologies for purposes of border management, and will follow closely the developments on this matter.

In line with the EDPB Strategy 2021-2023, the Board will continue to monitor new and emerging technologies, such as facial recognition, and their potential impact on the fundamental rights and daily lives of individuals, and will help to shape Europe's digital future in line with our common values and rules, while continuing to work with other regulators and policymakers to promote regulatory coherence and enhanced protection for individuals.

Yours sincerely,



Andrea Jelinek

**Andrea Jelinek**  
Chair of the European Data Protection Board

rue Wiertz, 60  
1047 Brussels

Ms. Estelle Massé  
Senior Policy Analyst  
Access Now

19 May 2021

**Sent by email only**

Ref: OUT2021-0085

**RE: Clarification on the process to identify a controller's main establishment under the GDPR**

Dear Ms Massé,

I would like to thank you for your letter of 9 April 2021 outlining your questions in relation to the Article 29 Working Party Guidelines for identifying a controller or processor's lead supervisory authority endorsed by the European Data Protection Board.

The importance of the efficient functioning of the cooperation and consistency mechanism is reflected in the EDPB Strategy 2021- 2023 as well as in the current EDPB work program.

The Guidelines for identifying a controller or processor's lead supervisory authority were adopted on 13 December 2016 following careful consideration of relevant factors for the determination of the main establishment and revised and adopted on 5 April 2017 by the members of the WP29. The EDPB members then agreed upon the endorsement of the revised version on 25 May 2018. As is the case with all guidance by the EDPB, we are permanently monitoring the necessity of reviewing also these guidelines and incorporating additional factors, and we will do so, if necessary.

While the EDPB cannot comment on possible ongoing investigations by its members, I would like to inform you that the Internal Market Information System (IMI), an information and communications system which facilitates the exchange of information between supervisory authorities for the GDPR cooperation and consistency procedures, does specifically enable any supervisory authority to express its views on competence at an early stage of such procedure launched by the supervisory authorities and/or initiate the dispute resolution mechanism as per Art. 65 GDPR.

The one-stop-shop mechanism ensures that the lead supervisory authority responsible for investigating cases against a particular controller considers the input of any concerned supervisory authority. The European Data Protection Board cannot make any statements regarding the main establishment of a particular controller, unless, for instance, it takes place within the framework of the dispute resolution mechanism (Art. 65 GDPR). Moreover, the competence to carry out investigations, according to Article 58.1 GDPR, is reserved for the national supervisory authorities.

Yours sincerely,



Andrea Jelinek

# Letters



Ms Mairead McGuinness  
European Commissioner for Financial services,  
Financial stability and Capital Markets Union  
Mr Didier Reynders  
European Commissioner for Justice  
***Sent by e-mail only***

Brussels, the 18 June 2021

REF: OUT2021-0105

Dear Commissioner McGuinness,  
Dear Commissioner Reynders,

In October 2020, the European Central Bank (ECB) issued the **Report on a digital euro**<sup>1</sup> aiming at consulting stakeholders, including the general public, on its project of a central bank digital currency (CBDC) in the Euro zone, which is expected to be available for retail payments ('digital euro'). In response to a significant decline in the role of cash as a means of payment, the digital euro would be an alternative to physical cash, not a substitute. As a digital form of the euro currency, the ECB want to "ensure that it was trusted from its inception and that this trust was maintained over time"<sup>1</sup>.

In April 2021, the ECB published a **feedback of the public consultation**<sup>2</sup>. The main finding was the very predominantly expressed preference by the stakeholders and the public for privacy<sup>3</sup> (43% as the most important feature)<sup>4</sup>. This result can be observed throughout the EU, population characteristics and in all categories of respondents (citizens, payment industry, merchants, NGOs, academics...). The majority of citizens declared they wanted "a digital euro focused on privacy and the protection of personal data, which can be used offline" (53%).

---

<sup>1</sup> [https://www.ecb.europa.eu/pub/pdf/other/Report\\_on\\_a\\_digital\\_euro~4d7268b458.en.pdf](https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf).

<sup>2</sup> <https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210414~ca3013c852.en.html>.

<sup>3</sup> "the privacy of payment data is considered the most important feature, ranging from full privacy of transactions to the possibility that only low-risk small transactions are private", feedback document, page 3.

<sup>4</sup> Although not representative of the EU population from a statistical point of view, the views collected nevertheless indicate issues that are important to the public.

In this context, the European Data Protection Board acknowledges that decisions regarding the launch of the project starting with a two-year exploratory phase will be held by mid-2021. The EDPB takes this opportunity to proactively advise the competent EU institutions on the privacy and personal data protection aspects of a digital euro, and inform the public debate in that regard, from the very early stage of decision making.

### **1. Background of the digital euro project and key data protection principles**

In the light of the views expressed by the citizens during the public consultation, the EDPB stresses that a very high standard of privacy and data protection is **crucial to reinforce the trust** of end users and shall be considered as a distinctive element in the offering of digital euro, representing a key factor of success of the project.

The EDPB acknowledges that the main architectural and design choices of a digital euro are not yet defined, while the ECB documents offer options between different features and modalities. In any chosen circumstance, the EDPB recalls the importance of taking in due account the compliance with the European data protection applicable framework<sup>5</sup> at an early stage of the project, pursuant to the key principle of data protection “**by design and by default**”, privacy and data protection principles should not be considered *a posteriori*, as a pure compliance exercise<sup>6</sup>. It shall be wired within core decisions on the outcome of the project, constituting a cornerstone of the final goal that the Eurosystem wants to achieve with respect to fundamental values of the European Union.

The EDPB recalls that the rights to privacy and to the protection of personal data are **fundamental rights** enshrined in the articles 7 and 8 of the Charter of Fundamental Rights of the European Union. They shall not be considered as absolute values, but carefully balanced with other rights at stake. The Court of Justice of the European Union has developed case law on the principles of necessity in a democratic society and proportionality of limitations to fundamental rights and principles, ensuring their appropriate protection<sup>7</sup>.

Under this light, the Report published by the European Central Bank offered a comprehensive overview of different interests at stake in relation to different design choices (innovation, privacy, financial stability, monetary policy, financial inclusion, etc.). However, new risks for rights and freedoms of individuals might arise from this project, while others already identified risks might be amplified (see part 2 below). Balance among these interests on one hand, and between them and privacy and personal data protection on the other hand, should be cautiously assessed in order to

---

<sup>5</sup> According to decision taken on personal data controllership, different legal instruments might come into play, mainly the Regulation (EU) no. 2016/679, General Data Protection Regulation, and/or the Regulation (EU) no. 2018/1725, 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.

<sup>6</sup> [https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and\\_en](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en) and [https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-design\\_en](https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-design_en).

<sup>7</sup> See for example: C-511/18 - La Quadrature du Net and Others, 6 Oct 2020; Tele2 Sverige AB (CJEU, C-203/15, ECLI:EU:C:2016:970); Ministerio Fiscal (CJEU, C-207/16, ECLI:EU:C:2018:788).

See also: EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, at: [19-12-19 edps\\_proportionality\\_guidelines2\\_en.pdf \(europa.eu\)](https://edps.europa.eu/data-protection/publications/opinions/privacy-design_en.pdf).

validate or adapt existing approaches in an innovative manner, with the final aim of minimising these risks.

Moreover, in the context of the digital euro initiative, the EDPB points out in particular to the **principle of data minimization**, according to which personal data shall be limited to what is necessary in relation to the purposes for which they are processed. **Purpose limitation**, according to which personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes, shall also be complied with in the context of a digital euro.

The EDPB wants to underline the **clear distinction** between an anonymous use of the digital euro<sup>8</sup> and the case where a natural person is identified or identifiable during its use, including if the data are pseudonymised, which requires the full compliance with GDPR. The choices made in that regard will of course also depend on the policy objectives pursued and on a number of public interests to be balanced. In any case, the architecture of the digital euro shall be designed to allow a privacy feature ranging from anonymisation, at least on part of the transactions, to a high level of pseudonymisation of the data<sup>9</sup>. The WP29 guidelines on anonymisation<sup>10</sup> are currently reviewed and the EDPB will be in a position to give more detailed advice on the subject matter from a technical point of view in the future<sup>11</sup>.

The EDPB considers that a **holistic assessment** of different aspects and fundamental rights at stake (financial and digital inclusion, privacy and data protection, freedom of movement, security) should be made to ensure that the digital euro project is in line with the values of the European Union and, in particular, with the protection of privacy and personal data.

## **2. Relevant privacy and data protection issues regarding the ‘architecture’ of the project**

The EDPB welcomes the overall objective of the project, namely increasing access to central bank currency in digital transactions enhancing innovation and pursing public interest in a well-functioning economy.

However, an inappropriate design of the forthcoming digital euro would bring **significant risks** under the data protection perspective. Relevant safeguards shall be put in place in order to avoid, for example, generalised tracking of user transactions throughout the payment system and to address and mitigate the risk of excessive interference in privacy of the persons concerned by both centralized entities and market operators.

In order to reach this objective, the identification of the end users should remain limited to what is necessary to the performance of regulatory obligations by obliged entities. Collection and access to

---

<sup>8</sup> As it is the case for physical cash.

<sup>9</sup> A thresholded approach could be based on the monetary value of the transaction. For example, low value transaction of less than €1000 could enjoy full privacy as they are unlikely to entail AML high risks. Another possible limitation could cover use outside the Euro area.

<sup>10</sup> [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf)

<sup>11</sup> See EDPB Work Program: [https://edpb.europa.eu/system/files/2021-03/edpb\\_workprogramme\\_2021-2022\\_en.pdf](https://edpb.europa.eu/system/files/2021-03/edpb_workprogramme_2021-2022_en.pdf)

personal data should be minimized to what is necessary to transfer the funds<sup>12</sup>, and security risks should be identified and mitigated.

Moreover, the EDPB understands that the digital euro **will have legal tender status** in the EU at the time of its issuance, which means, in regulatory terms, that it will be assimilated to euro banknotes within the meaning of Article 128 TFEU. Those are the only ones “to have the status of legal tender within the Union”. This means that a digital euro would be, in legal terms, an equivalent to cash. In this context, the EDPB considers that a digital euro shall have as far as possible ‘cash-like features’, in particular regarding the data protection aspects.

Concerning the ‘AML/CFT status’ of the new currency, the EDPB notes that regulators in this field assimilate central bank digital currencies to cash, considering it in this respect equivalent to any form of fiat currency issued by a central bank. Since both AML/CFT and data protection and privacy concerns are important concerns to be balanced in the design of the architecture of a digital euro, it follows that **physical cash is the relevant benchmark** to strike such a balance, for example by using a threshold-based approach, allowing full privacy for daily life transactions.

From an operational point of view, research conducted by the ECB shows that ensuring the adoption of appropriate pseudonymisation techniques in the use of digital cash under a certain threshold, while still ensuring that higher-value transactions are subject to mandatory AML/CFT checks, is technically challenging but could be considered<sup>13</sup>.

In this context, it seems to the EDPB that a modality offering **off-line transactions** (without internet connection to be accessible everywhere in the EU) anonymously or, in the lack of it, at least with a high level of pseudonymisation, is necessary to mitigate risks for rights and freedoms of data subjects.

Moreover, to the EDPB highlights that if a ‘decentralized approach’ were to be followed in that regard, the data should be tokenized<sup>14</sup> in order to avoid central monitoring of transactions, a good practice to consider would be to **store tokens locally** on an end-user device or digital wallet (like a smartphone or card to reach all types of public, and meeting the necessary software and hardware security conditions).

This token-based feature is compatible with interconnections to an **intermediary** distributing the digital euro, in order to refill the amounts of digital euro in the device or wallet, as it is currently the case for ATMs for example. During the interconnection, the transaction data would not be reported to the intermediary unless it reaches a given threshold. Moreover, the transactions that would be reported to the intermediary in charge of conducting AML/CFT due diligence and reporting have to be configured in at the minimum possible. Under such a framework, the on-boarding of end-users and monitoring of transactions by the ECB would not be necessary.

---

<sup>12</sup> According to article 4 of the PSD2 directive, ‘payment transaction’ means an act, initiated by the payer or on his behalf or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee.

<sup>13</sup><https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191217.en.pdf?3824c3f26ad2f928ceea370393cce785>.

<sup>14</sup> In other words, substitute a randomly generated identifier for a sensitive piece of data in order to prevent unauthorized access.

The technological and organisational features of the aforementioned token-based, decentralised approach should allow only and not prevent targeted identification of the parties, notably for AML/CFT purposes, avoiding any complete obfuscation of transactions, as it can be the case for some cryptocurrencies.

The EDPB considers that the **simplicity of the design**, its easy access and the use of current infrastructures (if an assessment shows that this does not come at the cost of privacy and data protection) of the new digital currency is also important in terms of financial inclusiveness.

### 3. Next steps on privacy and data protection

While data protection and privacy aspects need to be carefully evaluated within legislative processes, the EDPB notes that the digital euro project will entail an obligation to carry out a data protection impact assessment (DPIA) by the relevant controllers<sup>15</sup>. Any data controller involved in personal data processing operations shall then perform the assessment before the beginning of its operations and evaluate the need to consult the competent supervisory authority prior to processing if necessary<sup>16</sup>.

However, performing this analysis, as a high-level assessment on the overall project, would be of major help in correctly assessing and mitigating risks for rights and freedoms of data subjects and would provide key elements to be considered when deciding on the possible design and architectural scenarios.

In this context, we recommend that the EU body in charge of the design of the project performs such a **high-level impact assessment** on privacy and data protection during the exploratory phase.

Due to the importance of the initiative, the EDPB stands ready to **provide advice** upon formal or informal consultations by the ECB or by other EU institutions with the aim of ensuring at the same time the effectiveness and the less privacy-intrusive configuration, right after a decision to launch the project is taken, in order to provide a more granular compliance advice on the options considered.

Besides of the formal involvement of the EDPS, the EDPB would also like to express availability to **work at expert level** with the competent EU institutions from the early stage of development of the project, as well as during the exploratory phase.

For the European Data Protection Board,

The Chair

---

<sup>15</sup> See WP29, Guidance and [https://edps.europa.eu/data-protection/our-work/publications/guidelines/accountability-ground-provisional-guidance\\_en](https://edps.europa.eu/data-protection/our-work/publications/guidelines/accountability-ground-provisional-guidance_en).

<sup>16</sup>That is, if the DPIA indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in view of the available technologies and costs of implementation.

Andrea Jelinek

# Letters



## EDPB letter to the European institutions on the privacy and data protection aspects of a possible digital euro

Mr. Fabio Panetta  
European Central Bank  
*Sent by e-mail only*

Brussels, the 18 June 2021  
REF: OUT2021-0111

Dear Mr. Panetta,

In October 2020, the European Central Bank (ECB) issued the **Report on a digital euro**<sup>1</sup> aiming at consulting stakeholders, including the general public, on its project of a central bank digital currency (CBDC) in the Euro zone, which is expected to be available for retail payments ('digital euro'). In response to a significant decline in the role of cash as a means of payment, the digital euro would be an alternative to physical cash, not a substitute. As a digital form of the euro currency, the ECB want to "ensure that it was trusted from its inception and that this trust was maintained over time"<sup>1</sup>.

In April 2021, the ECB published a **feedback of the public consultation**<sup>2</sup>. The main finding was the very predominantly expressed preference by the stakeholders and the public for privacy<sup>3</sup> (43% as the most important feature)<sup>4</sup>. This result can be observed throughout the EU, population characteristics and in all categories of respondents (citizens, payment industry, merchants, NGOs, academics...). The majority of citizens declared they wanted "a digital euro focused on privacy and the protection of personal data, which can be used offline" (53%).

In this context, the European Data Protection Board acknowledges that decisions regarding the launch of the project starting with a two-year exploratory phase will be held by mid-2021. The EDPB takes this opportunity to proactively advise the competent EU institutions on the privacy and personal data

<sup>1</sup> [https://www.ecb.europa.eu/pub/pdf/other/Report\\_on\\_a\\_digital\\_euro~4d7268b458.en.pdf](https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf).

<sup>2</sup> <https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210414~ca3013c852.en.html>.

<sup>3</sup> "the privacy of payment data is considered the most important feature, ranging from full privacy of transactions to the possibility that only low-risk small transactions are private", feedback document, page 3.

<sup>4</sup> Although not representative of the EU population from a statistical point of view, the views collected nevertheless indicate issues that are important to the public.

protection aspects of a digital euro, and inform the public debate in that regard, from the very early stage of decision making.

## 1. Background of the digital euro project and key data protection principles

In the light of the views expressed by the citizens during the public consultation, the EDPB stresses that a very high standard of privacy and data protection is **crucial to reinforce the trust** of end users and shall be considered as a distinctive element in the offering of digital euro, representing a key factor of success of the project.

The EDPB acknowledges that the main architectural and design choices of a digital euro are not yet defined, while the ECB documents offer options between different features and modalities. In any chosen circumstance, the EDPB recalls the importance of taking in due account the compliance with the European data protection applicable framework<sup>5</sup> at an early stage of the project, pursuant to the key principle of data protection “**by design and by default**”, privacy and data protection principles should not be considered *a posteriori*, as a pure compliance exercise<sup>6</sup>. It shall be wired within core decisions on the outcome of the project, constituting a cornerstone of the final goal that the Eurosystem wants to achieve with respect to fundamental values of the European Union.

The EDPB recalls that the rights to privacy and to the protection of personal data are **fundamental rights** enshrined in the articles 7 and 8 of the Charter of Fundamental Rights of the European Union. They shall not be considered as absolute values, but carefully balanced with other rights at stake. The Court of Justice of the European Union has developed case law on the principles of necessity in a democratic society and proportionality of limitations to fundamental rights and principles, ensuring their appropriate protection<sup>7</sup>.

Under this light, the Report published by the European Central Bank offered a comprehensive overview of different interests at stake in relation to different design choices (innovation, privacy, financial stability, monetary policy, financial inclusion, etc.). However, new risks for rights and freedoms of individuals might arise from this project, while others already identified risks might be amplified (see part 2 below). Balance among these interests on one hand, and between them and privacy and personal data protection on the other hand, should be cautiously assessed in order to validate or adapt existing approaches in an innovative manner, with the final aim of minimising these risks.

---

<sup>5</sup> According to decision taken on personal data controllership, different legal instruments might come into play, mainly the Regulation (EU) no. 2016/679, General Data Protection Regulation, and/or the Regulation (EU) no. 2018/1725, 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.

<sup>6</sup> [https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and\\_en](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en) and [https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-design\\_en](https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-design_en).

<sup>7</sup> See for example: C-511/18 - La Quadrature du Net and Others, 6 Oct 2020; Tele2 Sverige AB (CJEU, C-203/15, ECLI:EU:C:2016:970); Ministerio Fiscal (CJEU, C-207/16, ECLI:EU:C:2018:788).

See also: EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, at: [19-12-19 edps\\_proportionality\\_guidelines2\\_en.pdf \(europa.eu\)](https://edps.europa.eu/data-protection/publications/opinions/privacy-design_en.pdf).

Moreover, in the context of the digital euro initiative, the EDPB points out in particular to the **principle of data minimization**, according to which personal data shall be limited to what is necessary in relation to the purposes for which they are processed. **Purpose limitation**, according to which personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes, shall also be complied with in the context of a digital euro.

The EDPB wants to underline the **clear distinction** between an anonymous use of the digital euro<sup>8</sup> and the case where a natural person is identified or identifiable during its use, including if the data are pseudonymised, which requires the full compliance with GDPR. The choices made in that regard will of course also depend on the policy objectives pursued and on a number of public interests to be balanced. In any case, the architecture of the digital euro shall be designed to allow a privacy feature ranging from anonymisation, at least on part of the transactions, to a high level of pseudonymisation of the data<sup>9</sup>. The WP29 guidelines on anonymisation<sup>10</sup> are currently reviewed and the EDPB will be in a position to give more detailed advice on the subject matter from a technical point of view in the future<sup>11</sup>.

The EDPB considers that **a holistic assessment** of different aspects and fundamental rights at stake (financial and digital inclusion, privacy and data protection, freedom of movement, security) should be made to ensure that the digital euro project is in line with the values of the European Union and, in particular, with the protection of privacy and personal data.

## 2. Relevant privacy and data protection issues regarding the ‘architecture’ of the project

The EDPB welcomes the overall objective of the project, namely increasing access to central bank currency in digital transactions enhancing innovation and pursing public interest in a well-functioning economy.

However, an inappropriate design of the forthcoming digital euro would bring **significant risks** under the data protection perspective. Relevant safeguards shall be put in place in order to avoid, for example, generalised tracking of user transactions throughout the payment system and to address and mitigate the risk of excessive interference in privacy of the persons concerned by both centralized entities and market operators.

In order to reach this objective, the identification of the end users should remain limited to what is necessary to the performance of regulatory obligations by obliged entities. Collection and access to personal data should be minimized to what is necessary to transfer the funds<sup>12</sup>, and security risks should be identified and mitigated.

---

<sup>8</sup> As it is the case for physical cash.

<sup>9</sup> A thresholded approach could be based on the monetary value of the transaction. For example, low value transaction of less than €1000 could enjoy full privacy as they are unlikely to entail AML high risks. Another possible limitation could cover use outside the Euro area.

<sup>10</sup> [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf)

<sup>11</sup> See EDPB Work Program: [https://edpb.europa.eu/system/files/2021-03/edpb\\_workprogramme\\_2021-2022\\_en.pdf](https://edpb.europa.eu/system/files/2021-03/edpb_workprogramme_2021-2022_en.pdf)

<sup>12</sup> According to article 4 of the PSD2 directive, ‘payment transaction’ means an act, initiated by the payer or on his behalf or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee.

Moreover, the EDPB understands that the digital euro **will have legal tender status** in the EU at the time of its issuance, which means, in regulatory terms, that it will be assimilated to euro banknotes within the meaning of Article 128 TFEU. Those are the only ones “to have the status of legal tender within the Union”. This means that a digital euro would be, in legal terms, an equivalent to cash. In this context, the EDPB considers that a digital euro shall have as far as possible ‘cash-like features’, in particular regarding the data protection aspects.

Concerning the ‘AML/CFT status’ of the new currency, the EDPB notes that regulators in this field assimilate central bank digital currencies to cash, considering it in this respect equivalent to any form of fiat currency issued by a central bank. Since both AML/CFT and data protection and privacy concerns are important concerns to be balanced in the design of the architecture of a digital euro, it follows that **physical cash is the relevant benchmark** to strike such a balance, for example by using a threshold-based approach, allowing full privacy for daily life transactions.

From an operational point of view, research conducted by the ECB shows that ensuring the adoption of appropriate pseudonymisation techniques in the use of digital cash under a certain threshold, while still ensuring that higher-value transactions are subject to mandatory AML/CFT checks, is technically challenging but could be considered<sup>13</sup>.

In this context, it seems to the EDPB that a modality offering **off-line transactions** (without internet connection to be accessible everywhere in the EU) anonymously or, in the lack of it, at least with a high level of pseudonymisation, is necessary to mitigate risks for rights and freedoms of data subjects.

Moreover, to the EDPB highlights that if a ‘decentralized approach’ were to be followed in that regard, the data should be tokenized<sup>14</sup> in order to avoid central monitoring of transactions, a good practice to consider would be to **store tokens locally** on an end-user device or digital wallet (like a smartphone or card to reach all types of public, and meeting the necessary software and hardware security conditions).

This token-based feature is compatible with interconnections to an **intermediary** distributing the digital euro, in order to refill the amounts of digital euro in the device or wallet, as it is currently the case for ATMs for example. During the interconnection, the transaction data would not be reported to the intermediary unless it reaches a given threshold. Moreover, the transactions that would be reported to the intermediary in charge of conducting AML/CFT due diligence and reporting have to be configured in at the minimum possible. Under such a framework, the on-boarding of end-users and monitoring of transactions by the ECB would not be necessary.

The technological and organisational features of the aforementioned token-based, decentralised approach should allow only and not prevent targeted identification of the parties, notably for AML/CFT purposes, avoiding any complete obfuscation of transactions, as it can be the case for some cryptocurrencies.

---

<sup>13</sup><https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191217.en.pdf?3824c3f26ad2f928ceea370393cce785>.

<sup>14</sup> In other words, substitute a randomly generated identifier for a sensitive piece of data in order to prevent unauthorized access.

The EDPB considers that the **simplicity of the design**, its easy access and the use of current infrastructures (if an assessment shows that this does not come at the cost of privacy and data protection) of the new digital currency is also important in terms of financial inclusiveness.

### 3. Next steps on privacy and data protection

While data protection and privacy aspects need to be carefully evaluated within legislative processes, the EDPB notes that the digital euro project will entail an obligation to carry out a data protection impact assessment (DPIA) by the relevant controllers<sup>15</sup>. Any data controller involved in personal data processing operations shall then perform the assessment before the beginning of its operations and evaluate the need to consult the competent supervisory authority prior to processing if necessary<sup>16</sup>.

However, performing this analysis, as a high-level assessment on the overall project, would be of major help in correctly assessing and mitigating risks for rights and freedoms of data subjects and would provide key elements to be considered when deciding on the possible design and architectural scenarios.

In this context, we recommend that the EU body in charge of the design of the project performs such a **high-level impact assessment** on privacy and data protection during the exploratory phase.

Due to the importance of the initiative, the EDPB stands ready to **provide advice** upon formal or informal consultations by the ECB or by other EU institutions with the aim of ensuring at the same time the effectiveness and the less privacy-intrusive configuration, right after a decision to launch the project is taken, in order to provide a more granular compliance advice on the options considered.

Besides of the formal involvement of the EDPS, the EDPB would also like to express availability to **work at expert level** with the competent EU institutions from the early stage of development of the project, as well as during the exploratory phase.

For the European Data Protection Board,

The Chair



Andrea Jelinek

---

<sup>15</sup> See WP29, Guidance and [https://edps.europa.eu/data-protection/our-work/publications/guidelines/accountability-ground-provisional-guidance\\_en](https://edps.europa.eu/data-protection/our-work/publications/guidelines/accountability-ground-provisional-guidance_en).

<sup>16</sup>That is, if the DPIA indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in view of the available technologies and costs of implementation.

# Letters



## EDPB letter to the European institutions on the privacy and data protection aspects of a possible digital euro

ECON Committee of the European Parliament

JURI Committee of the European Parliament

*Sent by e-mail only*

Brussels, the 18 June 2021

REF: OUT2021-0112

Dear Sir/Madam,

In October 2020, the European Central Bank (ECB) issued the **Report on a digital euro**<sup>1</sup> aiming at consulting stakeholders, including the general public, on its project of a central bank digital currency (CBDC) in the Euro zone, which is expected to be available for retail payments ('digital euro'). In response to a significant decline in the role of cash as a means of payment, the digital euro would be an alternative to physical cash, not a substitute. As a digital form of the euro currency, the ECB want to "ensure that it was trusted from its inception and that this trust was maintained over time"<sup>1</sup>.

In April 2021, the ECB published a **feedback of the public consultation**<sup>2</sup>. The main finding was the very predominantly expressed preference by the stakeholders and the public for privacy<sup>3</sup> (43% as the most important feature)<sup>4</sup>. This result can be observed throughout the EU, population characteristics and in all categories of respondents (citizens, payment industry, merchants, NGOs, academics...). The majority of citizens declared they wanted "a digital euro focused on privacy and the protection of personal data, which can be used offline" (53%).

In this context, the European Data Protection Board acknowledges that decisions regarding the launch of the project starting with a two-year exploratory phase will be held by mid-2021. The EDPB takes this opportunity to proactively advise the competent EU institutions on the privacy and personal data

<sup>1</sup> [https://www.ecb.europa.eu/pub/pdf/other/Report\\_on\\_a\\_digital\\_euro~4d7268b458.en.pdf](https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf).

<sup>2</sup> <https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210414~ca3013c852.en.html>.

<sup>3</sup> "the privacy of payment data is considered the most important feature, ranging from full privacy of transactions to the possibility that only low-risk small transactions are private", feedback document, page 3.

<sup>4</sup> Although not representative of the EU population from a statistical point of view, the views collected nevertheless indicate issues that are important to the public.

protection aspects of a digital euro, and inform the public debate in that regard, from the very early stage of decision making.

## 1. Background of the digital euro project and key data protection principles

In the light of the views expressed by the citizens during the public consultation, the EDPB stresses that a very high standard of privacy and data protection is **crucial to reinforce the trust** of end users and shall be considered as a distinctive element in the offering of digital euro, representing a key factor of success of the project.

The EDPB acknowledges that the main architectural and design choices of a digital euro are not yet defined, while the ECB documents offer options between different features and modalities. In any chosen circumstance, the EDPB recalls the importance of taking in due account the compliance with the European data protection applicable framework<sup>5</sup> at an early stage of the project, pursuant to the key principle of data protection “**by design and by default**”, privacy and data protection principles should not be considered *a posteriori*, as a pure compliance exercise<sup>6</sup>. It shall be wired within core decisions on the outcome of the project, constituting a cornerstone of the final goal that the Eurosystem wants to achieve with respect to fundamental values of the European Union.

The EDPB recalls that the rights to privacy and to the protection of personal data are **fundamental rights** enshrined in the articles 7 and 8 of the Charter of Fundamental Rights of the European Union. They shall not be considered as absolute values, but carefully balanced with other rights at stake. The Court of Justice of the European Union has developed case law on the principles of necessity in a democratic society and proportionality of limitations to fundamental rights and principles, ensuring their appropriate protection<sup>7</sup>.

Under this light, the Report published by the European Central Bank offered a comprehensive overview of different interests at stake in relation to different design choices (innovation, privacy, financial stability, monetary policy, financial inclusion, etc.). However, new risks for rights and freedoms of individuals might arise from this project, while others already identified risks might be amplified (see part 2 below). Balance among these interests on one hand, and between them and privacy and personal data protection on the other hand, should be cautiously assessed in order to validate or adapt existing approaches in an innovative manner, with the final aim of minimising these risks.

---

<sup>5</sup> According to decision taken on personal data controllership, different legal instruments might come into play, mainly the Regulation (EU) no. 2016/679, General Data Protection Regulation, and/or the Regulation (EU) no. 2018/1725, 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.

<sup>6</sup> [https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and\\_en](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en) and [https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-design\\_en](https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-design_en).

<sup>7</sup> See for example: C-511/18 - La Quadrature du Net and Others, 6 Oct 2020; Tele2 Sverige AB (CJEU, C-203/15, ECLI:EU:C:2016:970); Ministerio Fiscal (CJEU, C-207/16, ECLI:EU:C:2018:788).

See also: EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, at: [19-12-19 edps\\_proportionality\\_guidelines2\\_en.pdf \(europa.eu\)](https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-design_en).

Moreover, in the context of the digital euro initiative, the EDPB points out in particular to the **principle of data minimization**, according to which personal data shall be limited to what is necessary in relation to the purposes for which they are processed. **Purpose limitation**, according to which personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes, shall also be complied with in the context of a digital euro.

The EDPB wants to underline the **clear distinction** between an anonymous use of the digital euro<sup>8</sup> and the case where a natural person is identified or identifiable during its use, including if the data are pseudonymised, which requires the full compliance with GDPR. The choices made in that regard will of course also depend on the policy objectives pursued and on a number of public interests to be balanced. In any case, the architecture of the digital euro shall be designed to allow a privacy feature ranging from anonymisation, at least on part of the transactions, to a high level of pseudonymisation of the data<sup>9</sup>. The WP29 guidelines on anonymisation<sup>10</sup> are currently reviewed and the EDPB will be in a position to give more detailed advice on the subject matter from a technical point of view in the future<sup>11</sup>.

The EDPB considers that **a holistic assessment** of different aspects and fundamental rights at stake (financial and digital inclusion, privacy and data protection, freedom of movement, security) should be made to ensure that the digital euro project is in line with the values of the European Union and, in particular, with the protection of privacy and personal data.

## **2. Relevant privacy and data protection issues regarding the ‘architecture’ of the project**

The EDPB welcomes the overall objective of the project, namely increasing access to central bank currency in digital transactions enhancing innovation and pursing public interest in a well-functioning economy.

However, an inappropriate design of the forthcoming digital euro would bring **significant risks** under the data protection perspective. Relevant safeguards shall be put in place in order to avoid, for example, generalised tracking of user transactions throughout the payment system and to address and mitigate the risk of excessive interference in privacy of the persons concerned by both centralized entities and market operators.

In order to reach this objective, the identification of the end users should remain limited to what is necessary to the performance of regulatory obligations by obliged entities. Collection and access to personal data should be minimized to what is necessary to transfer the funds<sup>12</sup>, and security risks should be identified and mitigated.

---

<sup>8</sup> As it is the case for physical cash.

<sup>9</sup> A thresholded approach could be based on the monetary value of the transaction. For example, low value transaction of less than €1000 could enjoy full privacy as they are unlikely to entail AML high risks. Another possible limitation could cover use outside the Euro area.

<sup>10</sup> [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf)

<sup>11</sup> See EDPB Work Program: [https://edpb.europa.eu/system/files/2021-03/edpb\\_workprogramme\\_2021-2022\\_en.pdf](https://edpb.europa.eu/system/files/2021-03/edpb_workprogramme_2021-2022_en.pdf)

<sup>12</sup> According to article 4 of the PSD2 directive, ‘payment transaction’ means an act, initiated by the payer or on his behalf or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee.

Moreover, the EDPB understands that the digital euro **will have legal tender status** in the EU at the time of its issuance, which means, in regulatory terms, that it will be assimilated to euro banknotes within the meaning of Article 128 TFEU. Those are the only ones “to have the status of legal tender within the Union”. This means that a digital euro would be, in legal terms, an equivalent to cash. In this context, the EDPB considers that a digital euro shall have as far as possible ‘cash-like features’, in particular regarding the data protection aspects.

Concerning the ‘AML/CFT status’ of the new currency, the EDPB notes that regulators in this field assimilate central bank digital currencies to cash, considering it in this respect equivalent to any form of fiat currency issued by a central bank. Since both AML/CFT and data protection and privacy concerns are important concerns to be balanced in the design of the architecture of a digital euro, it follows that **physical cash is the relevant benchmark** to strike such a balance, for example by using a threshold-based approach, allowing full privacy for daily life transactions.

From an operational point of view, research conducted by the ECB shows that ensuring the adoption of appropriate pseudonymisation techniques in the use of digital cash under a certain threshold, while still ensuring that higher-value transactions are subject to mandatory AML/CFT checks, is technically challenging but could be considered<sup>13</sup>.

In this context, it seems to the EDPB that a modality offering **off-line transactions** (without internet connection to be accessible everywhere in the EU) anonymously or, in the lack of it, at least with a high level of pseudonymisation, is necessary to mitigate risks for rights and freedoms of data subjects.

Moreover, to the EDPB highlights that if a ‘decentralized approach’ were to be followed in that regard, the data should be tokenized<sup>14</sup> in order to avoid central monitoring of transactions, a good practice to consider would be to **store tokens locally** on an end-user device or digital wallet (like a smartphone or card to reach all types of public, and meeting the necessary software and hardware security conditions).

This token-based feature is compatible with interconnections to an **intermediary** distributing the digital euro, in order to refill the amounts of digital euro in the device or wallet, as it is currently the case for ATMs for example. During the interconnection, the transaction data would not be reported to the intermediary unless it reaches a given threshold. Moreover, the transactions that would be reported to the intermediary in charge of conducting AML/CFT due diligence and reporting have to be configured in at the minimum possible. Under such a framework, the on-boarding of end-users and monitoring of transactions by the ECB would not be necessary.

The technological and organisational features of the aforementioned token-based, decentralised approach should allow only and not prevent targeted identification of the parties, notably for AML/CFT purposes, avoiding any complete obfuscation of transactions, as it can be the case for some cryptocurrencies.

---

<sup>13</sup><https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191217.en.pdf?3824c3f26ad2f928ceea370393cce785>.

<sup>14</sup> In other words, substitute a randomly generated identifier for a sensitive piece of data in order to prevent unauthorized access.

The EDPB considers that the **simplicity of the design**, its easy access and the use of current infrastructures (if an assessment shows that this does not come at the cost of privacy and data protection) of the new digital currency is also important in terms of financial inclusiveness.

### 3. Next steps on privacy and data protection

While data protection and privacy aspects need to be carefully evaluated within legislative processes, the EDPB notes that the digital euro project will entail an obligation to carry out a data protection impact assessment (DPIA) by the relevant controllers<sup>15</sup>. Any data controller involved in personal data processing operations shall then perform the assessment before the beginning of its operations and evaluate the need to consult the competent supervisory authority prior to processing if necessary<sup>16</sup>.

However, performing this analysis, as a high-level assessment on the overall project, would be of major help in correctly assessing and mitigating risks for rights and freedoms of data subjects and would provide key elements to be considered when deciding on the possible design and architectural scenarios.

In this context, we recommend that the EU body in charge of the design of the project performs such a **high-level impact assessment** on privacy and data protection during the exploratory phase.

Due to the importance of the initiative, the EDPB stands ready to **provide advice** upon formal or informal consultations by the ECB or by other EU institutions with the aim of ensuring at the same time the effectiveness and the less privacy-intrusive configuration, right after a decision to launch the project is taken, in order to provide a more granular compliance advice on the options considered.

Besides of the formal involvement of the EDPS, the EDPB would also like to express availability to **work at expert level** with the competent EU institutions from the early stage of development of the project, as well as during the exploratory phase.

For the European Data Protection Board,

The Chair



(Andrea Jelinek)

---

<sup>15</sup> See WP29, Guidance and [https://edps.europa.eu/data-protection/our-work/publications/guidelines/accountability-ground-provisional-guidance\\_en](https://edps.europa.eu/data-protection/our-work/publications/guidelines/accountability-ground-provisional-guidance_en).

<sup>16</sup>That is, if the DPIA indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in view of the available technologies and costs of implementation.

# Letters



## EDPB letter to the European institutions on the privacy and data protection aspects of a possible digital euro

Slovenian Presidency of the Council

*Sent by e-mail only*

Brussels, the 18 June 2021

REF: OUT2021-0113

Dear Sir/Madam,

In October 2020, the European Central Bank (ECB) issued the **Report on a digital euro**<sup>1</sup> aiming at consulting stakeholders, including the general public, on its project of a central bank digital currency (CBDC) in the Euro zone, which is expected to be available for retail payments ('digital euro'). In response to a significant decline in the role of cash as a means of payment, the digital euro would be an alternative to physical cash, not a substitute. As a digital form of the euro currency, the ECB want to "ensure that it was trusted from its inception and that this trust was maintained over time"<sup>1</sup>.

In April 2021, the ECB published a **feedback of the public consultation**<sup>2</sup>. The main finding was the very predominantly expressed preference by the stakeholders and the public for privacy<sup>3</sup> (43% as the most important feature)<sup>4</sup>. This result can be observed throughout the EU, population characteristics and in all categories of respondents (citizens, payment industry, merchants, NGOs, academics...). The majority of citizens declared they wanted "a digital euro focused on privacy and the protection of personal data, which can be used offline" (53%).

In this context, the European Data Protection Board acknowledges that decisions regarding the launch of the project starting with a two-year exploratory phase will be held by mid-2021. The EDPB takes this opportunity to proactively advise the competent EU institutions on the privacy and personal data

---

<sup>1</sup> [https://www.ecb.europa.eu/pub/pdf/other/Report\\_on\\_a\\_digital\\_euro~4d7268b458.en.pdf](https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf).

<sup>2</sup> <https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210414~ca3013c852.en.html>.

<sup>3</sup> "the privacy of payment data is considered the most important feature, ranging from full privacy of transactions to the possibility that only low-risk small transactions are private", feedback document, page 3.

<sup>4</sup> Although not representative of the EU population from a statistical point of view, the views collected nevertheless indicate issues that are important to the public.

protection aspects of a digital euro, and inform the public debate in that regard, from the very early stage of decision making.

### **1. Background of the digital euro project and key data protection principles**

In the light of the views expressed by the citizens during the public consultation, the EDPB stresses that a very high standard of privacy and data protection is **crucial to reinforce the trust** of end users and shall be considered as a distinctive element in the offering of digital euro, representing a key factor of success of the project.

The EDPB acknowledges that the main architectural and design choices of a digital euro are not yet defined, while the ECB documents offer options between different features and modalities. In any chosen circumstance, the EDPB recalls the importance of taking in due account the compliance with the European data protection applicable framework<sup>5</sup> at an early stage of the project, pursuant to the key principle of data protection “**by design and by default**”, privacy and data protection principles should not be considered *a posteriori*, as a pure compliance exercise<sup>6</sup>. It shall be wired within core decisions on the outcome of the project, constituting a cornerstone of the final goal that the Eurosystem wants to achieve with respect to fundamental values of the European Union.

The EDPB recalls that the rights to privacy and to the protection of personal data are **fundamental rights** enshrined in the articles 7 and 8 of the Charter of Fundamental Rights of the European Union. They shall not be considered as absolute values, but carefully balanced with other rights at stake. The Court of Justice of the European Union has developed case law on the principles of necessity in a democratic society and proportionality of limitations to fundamental rights and principles, ensuring their appropriate protection<sup>7</sup>.

Under this light, the Report published by the European Central Bank offered a comprehensive overview of different interests at stake in relation to different design choices (innovation, privacy, financial stability, monetary policy, financial inclusion, etc.). However, new risks for rights and freedoms of individuals might arise from this project, while others already identified risks might be amplified (see part 2 below). Balance among these interests on one hand, and between them and privacy and personal data protection on the other hand, should be cautiously assessed in order to validate or adapt existing approaches in an innovative manner, with the final aim of minimising these risks.

---

<sup>5</sup> According to decision taken on personal data controllership, different legal instruments might come into play, mainly the Regulation (EU) no. 2016/679, General Data Protection Regulation, and/or the Regulation (EU) no. 2018/1725, 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.

<sup>6</sup> [https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and\\_en](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en) and [https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-design\\_en](https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-design_en).

<sup>7</sup> See for example: C-511/18 - La Quadrature du Net and Others, 6 Oct 2020; Tele2 Sverige AB (CJEU, C-203/15, ECLI:EU:C:2016:970); Ministerio Fiscal (CJEU, C-207/16, ECLI:EU:C:2018:788).

See also: EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, at: [19-12-19 edps\\_proportionality\\_guidelines2\\_en.pdf \(europa.eu\)](https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-design_en).

Moreover, in the context of the digital euro initiative, the EDPB points out in particular to the **principle of data minimization**, according to which personal data shall be limited to what is necessary in relation to the purposes for which they are processed. **Purpose limitation**, according to which personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes, shall also be complied with in the context of a digital euro.

The EDPB wants to underline the **clear distinction** between an anonymous use of the digital euro<sup>8</sup> and the case where a natural person is identified or identifiable during its use, including if the data are pseudonymised, which requires the full compliance with GDPR. The choices made in that regard will of course also depend on the policy objectives pursued and on a number of public interests to be balanced. In any case, the architecture of the digital euro shall be designed to allow a privacy feature ranging from anonymisation, at least on part of the transactions, to a high level of pseudonymisation of the data<sup>9</sup>. The WP29 guidelines on anonymisation<sup>10</sup> are currently reviewed and the EDPB will be in a position to give more detailed advice on the subject matter from a technical point of view in the future<sup>11</sup>.

The EDPB considers that **a holistic assessment** of different aspects and fundamental rights at stake (financial and digital inclusion, privacy and data protection, freedom of movement, security) should be made to ensure that the digital euro project is in line with the values of the European Union and, in particular, with the protection of privacy and personal data.

## 2. Relevant privacy and data protection issues regarding the ‘architecture’ of the project

The EDPB welcomes the overall objective of the project, namely increasing access to central bank currency in digital transactions enhancing innovation and pursing public interest in a well-functioning economy.

However, an inappropriate design of the forthcoming digital euro would bring **significant risks** under the data protection perspective. Relevant safeguards shall be put in place in order to avoid, for example, generalised tracking of user transactions throughout the payment system and to address and mitigate the risk of excessive interference in privacy of the persons concerned by both centralized entities and market operators.

In order to reach this objective, the identification of the end users should remain limited to what is necessary to the performance of regulatory obligations by obliged entities. Collection and access to personal data should be minimized to what is necessary to transfer the funds<sup>12</sup>, and security risks should be identified and mitigated.

---

<sup>8</sup> As it is the case for physical cash.

<sup>9</sup> A thresholded approach could be based on the monetary value of the transaction. For example, low value transaction of less than €1000 could enjoy full privacy as they are unlikely to entail AML high risks. Another possible limitation could cover use outside the Euro area.

<sup>10</sup> [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf)

<sup>11</sup> See EDPB Work Program: [https://edpb.europa.eu/system/files/2021-03/edpb\\_workprogramme\\_2021-2022\\_en.pdf](https://edpb.europa.eu/system/files/2021-03/edpb_workprogramme_2021-2022_en.pdf)

<sup>12</sup> According to article 4 of the PSD2 directive, ‘payment transaction’ means an act, initiated by the payer or on his behalf or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee.

Moreover, the EDPB understands that the digital euro **will have legal tender status** in the EU at the time of its issuance, which means, in regulatory terms, that it will be assimilated to euro banknotes within the meaning of Article 128 TFEU. Those are the only ones “to have the status of legal tender within the Union”. This means that a digital euro would be, in legal terms, an equivalent to cash. In this context, the EDPB considers that a digital euro shall have as far as possible ‘cash-like features’, in particular regarding the data protection aspects.

Concerning the ‘AML/CFT status’ of the new currency, the EDPB notes that regulators in this field assimilate central bank digital currencies to cash, considering it in this respect equivalent to any form of fiat currency issued by a central bank. Since both AML/CFT and data protection and privacy concerns are important concerns to be balanced in the design of the architecture of a digital euro, it follows that **physical cash is the relevant benchmark** to strike such a balance, for example by using a threshold-based approach, allowing full privacy for daily life transactions.

From an operational point of view, research conducted by the ECB shows that ensuring the adoption of appropriate pseudonymisation techniques in the use of digital cash under a certain threshold, while still ensuring that higher-value transactions are subject to mandatory AML/CFT checks, is technically challenging but could be considered<sup>13</sup>.

In this context, it seems to the EDPB that a modality offering **off-line transactions** (without internet connection to be accessible everywhere in the EU) anonymously or, in the lack of it, at least with a high level of pseudonymisation, is necessary to mitigate risks for rights and freedoms of data subjects.

Moreover, to the EDPB highlights that if a ‘decentralized approach’ were to be followed in that regard, the data should be tokenized<sup>14</sup> in order to avoid central monitoring of transactions, a good practice to consider would be to **store tokens locally** on an end-user device or digital wallet (like a smartphone or card to reach all types of public, and meeting the necessary software and hardware security conditions).

This token-based feature is compatible with interconnections to an **intermediary** distributing the digital euro, in order to refill the amounts of digital euro in the device or wallet, as it is currently the case for ATMs for example. During the interconnection, the transaction data would not be reported to the intermediary unless it reaches a given threshold. Moreover, the transactions that would be reported to the intermediary in charge of conducting AML/CFT due diligence and reporting have to be configured in at the minimum possible. Under such a framework, the on-boarding of end-users and monitoring of transactions by the ECB would not be necessary.

The technological and organisational features of the aforementioned token-based, decentralised approach should allow only and not prevent targeted identification of the parties, notably for AML/CFT purposes, avoiding any complete obfuscation of transactions, as it can be the case for some cryptocurrencies.

---

<sup>13</sup><https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191217.en.pdf?3824c3f26ad2f928ceea370393cce785>.

<sup>14</sup> In other words, substitute a randomly generated identifier for a sensitive piece of data in order to prevent unauthorized access.

The EDPB considers that the **simplicity of the design**, its easy access and the use of current infrastructures (if an assessment shows that this does not come at the cost of privacy and data protection) of the new digital currency is also important in terms of financial inclusiveness.

### 3. Next steps on privacy and data protection

While data protection and privacy aspects need to be carefully evaluated within legislative processes, the EDPB notes that the digital euro project will entail an obligation to carry out a data protection impact assessment (DPIA) by the relevant controllers<sup>15</sup>. Any data controller involved in personal data processing operations shall then perform the assessment before the beginning of its operations and evaluate the need to consult the competent supervisory authority prior to processing if necessary<sup>16</sup>.

However, performing this analysis, as a high-level assessment on the overall project, would be of major help in correctly assessing and mitigating risks for rights and freedoms of data subjects and would provide key elements to be considered when deciding on the possible design and architectural scenarios.

In this context, we recommend that the EU body in charge of the design of the project performs such a **high-level impact assessment** on privacy and data protection during the exploratory phase.

Due to the importance of the initiative, the EDPB stands ready to **provide advice** upon formal or informal consultations by the ECB or by other EU institutions with the aim of ensuring at the same time the effectiveness and the less privacy-intrusive configuration, right after a decision to launch the project is taken, in order to provide a more granular compliance advice on the options considered.

Besides of the formal involvement of the EDPS, the EDPB would also like to express availability to **work at expert level** with the competent EU institutions from the early stage of development of the project, as well as during the exploratory phase.

For the European Data Protection Board,

The Chair



(Andrea Jelinek)

---

<sup>15</sup> See WP29, Guidance and [https://edps.europa.eu/data-protection/our-work/publications/guidelines/accountability-ground-provisional-guidance\\_en](https://edps.europa.eu/data-protection/our-work/publications/guidelines/accountability-ground-provisional-guidance_en).

<sup>16</sup>That is, if the DPIA indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in view of the available technologies and costs of implementation.



# Letters



Brussels, 3 March 2022

Ref: OUT2022-0011

***Sent by e-mail only***

Dear Ms. Pachl,

With respect to your letter dated 21 December 2021, first let me express our appreciation for BEUC's efforts aimed at protecting consumer rights and ensuring that the ad-tech industry respects the EU data protection laws. I would also like to thank you for your attention dedicated to our recent work on EU digital files, including Digital Markets Act and Digital Services Act.

I would like to underline that the European Data Protection Board is committed to ensuring consistent application of the General Data Protection Regulation, including in the ad-tech sector. As indicated in my letter to BEUC dated 18 June 2020<sup>1</sup>, while the EDPB lacks the required competence to launch investigations, as this competence lies with the relevant national supervisory authorities, the topic of privacy in the ad-tech industry is assigned to the relevant EDPB Expert Subgroups. Thanks to the work we have conducted in this context, we have adopted documents such as the Guidelines 8/2020 on the targeting of social media users<sup>2</sup> and the updated Guidelines 05/2020 on consent under Regulation 2016/679<sup>3</sup> that are relevant to building a uniform approach to this matter. We are also monitoring relevant legislative procedures and actively collaborating with the Consumer Protection Cooperation Network.

The EDPB's actions to support the enforcement of the GDPR, at the core of the second pillar of our Strategy for 2021-2023<sup>4</sup>, is also demonstrated by the creation of projects like the Support Pool of Experts and the Coordinated Enforcement Framework<sup>5</sup>. In parallel, EDPB Expert Subgroups also serve

---

<sup>1</sup> Available at: [https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-response-monique-goyens-ursula-pachl-beuc\\_en](https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-response-monique-goyens-ursula-pachl-beuc_en).

<sup>2</sup> The guidelines were adopted in their final version after public consultation on 13 April 2021 and are available at: [https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82020-targeting-social-media-users\\_en](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82020-targeting-social-media-users_en).

<sup>3</sup> See in particular paragraphs 38-41 and 86 of the updated guidelines. Available at: [https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679\\_en](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en).

<sup>4</sup> Available at: [https://edpb.europa.eu/our-work-tools/our-documents/strategy-work-programme/edpb-strategy-2021-2023\\_en](https://edpb.europa.eu/our-work-tools/our-documents/strategy-work-programme/edpb-strategy-2021-2023_en).

<sup>5</sup> Further information is available here: [https://edpb.europa.eu/our-work-tools/support-cooperation-and-enforcement/gdpr-cooperation-and-enforcement\\_en](https://edpb.europa.eu/our-work-tools/support-cooperation-and-enforcement/gdpr-cooperation-and-enforcement_en).

as a useful forum for the national supervisory authorities to coordinate, cooperate and exchange experiences.

I would like to reassure you that your letter has been circulated within all the EDPB members.

Yours sincerely,



Andrea Jelinek



**Andrea Jelinek**  
Chair of the European Data Protection Board

rue Wiertz, 60  
1047 Brussels

# Letters



Brussels, 6 April 2022

Ref: OUT2022-0026

***Sent by e-mail only***

Dear President of the Belgian Chamber of Representatives Tillieux,

Dear Prime Minister De Croo,

Dear State Secretary Michel,

CC: Vice-President Jourová,  
Commissioner Reynders,

In its Plenary meetings of 22 February 2022 and 14 March 2022, the European Data Protection Board (EDPB) was made aware of legislative developments in Belgium that may affect one of our members, the Belgian Data Protection Authority (*Gegevensbeschermingsautoriteit* (GBA) / *L'Autorité de protection des données* (APD)). With this letter, the EDPB would like to express its concern about these developments, particularly where they may negatively impact the stability and the independent functioning of the GBA/APD and thereby the consistent application of the GDPR. For that reason, despite the fact that it is not its role to assess how a specific national legislation ensures compliance with Article 52 GDPR, the EDPB considers it important to bring this matter to your attention.

In particular, these legislative developments concern a draft law aimed at reforming the Belgian law of 3 December 2017 establishing the GBA/APD (AH-2022-0020). This draft law was approved by the Belgian Council of Ministers on 28 January 2022. In the draft law, several changes are introduced to the structure, the governance and the staff of the GBA/APD. Most notably, the draft law aims to:

- **interrupt the current mandate** of all of the GBA/APD's external members<sup>1</sup>, who will change status and no longer take part in deliberations within the Litigation Chamber and the Knowledge Centre;
- **add new grounds for dismissal** of members, if they obstruct the proper functioning of the GBA/APD or if they fail to respect the collegiality of the executive committee;
- and **strengthen parliamentary oversight** over the functioning of the GBA/APD, for instance by requiring parliamentary approval of the GBA/APD's strategic plan and its internal Rules of Procedure, or by providing for a procedure of evaluation of the members which can already start one year before the end of their mandate.

<sup>1</sup> The Belgian DPA Act uses both "external members" and "members" when referring to the members of the Litigation Chamber in charge of enforcement and adoption of corrective measures and the Knowledge Centre, in charge of the adoption of opinions on new Belgian legislative and administrative measures relating to data protection. Despite the fact that they are not employed on a full-time basis, these individuals are considered to be formal members of the GBA/APD as they have decisional power for the adoption of decisions or opinions.

In addition to this reform, the Belgian Government proposed another draft legislation,<sup>2</sup> providing that the GBA/APD is to make use of a **mandatory shared service centre for the execution of tasks** related to HR, IT, security of information, finance and procurement. As the externalisation of these resources, which are directly linked to the autonomous functioning of the GBA/APD, will thus be imposed on the GBA/APD without prior consultation, the draft legislation would further undermine the independence of the GBA/APD in light of Article 52 GDPR — e.g. with regard to the recruitment, administration and management of its internal personnel.

First and foremost, the EDPB recalls that independent supervision is an essential element of the fundamental right to data protection under Article 8(3) of the EU Charter of Fundamental Rights and Article 16(2) of the EU Treaty. This requirement has been applied strictly by the Court of Justice, which has condemned the lack of independence of authorities judgments concerning infringement proceedings against Germany, Austria and Hungary,<sup>3</sup> and its opinion concerning the failure of Canada to provide for independent supervision in the draft EU-Canada PNR Agreement.<sup>4</sup> Most notably, the Court has specifically ruled that “it is not permissible for a Member State to require that a supervisory authority vacates its office before serving its full term”, as the threat of such termination could lead to “a form of prior compliance with the political authority, which is incompatible with the requirement of independence.” This even holds true in case “premature termination of the term served comes about as a result of the restructuring or changing of the institutional model.”<sup>5</sup>

The EDPB also recalls that the GDPR specifically requires that each supervisory authority shall act with complete independence in performing its tasks and exercising its powers (Article 52(1) GDPR). This entails, amongst other things, that members of each supervisory authority shall, in the performance of their tasks and exercise remain free from external influence (Article 52(2) GDPR), that Member States shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned (Article 52(5) GDPR) and that Member States shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers (Article 52(4) GDPR).

Seen in this context, the EDPB is concerned about the impact that the proposed reforms may have on the independent functioning of the Belgian Data Protection Authority. The EDPB considers that the proposals to **interrupt the current mandate** of the GBA/APD’s external members may be at odds with the abovementioned case law of the Court of Justice.<sup>6</sup> Furthermore, the EDPB considers that the **added grounds of dismissal** in the draft law may be inconsistent with Article 53(4) GDPR, which clearly states that “a member shall be dismissed only in cases of serious misconduct or if the member no longer

---

<sup>2</sup> According to the Opinion of the GBA/APD on the new draft legislation. Opinion on preliminary draft law amending the Act of 3 December 2017 establishing the Data Protection Authority (AH-2022-0020), paras. 3 and 24, see: <https://www.autoriteprotectiondonnees.be/publications/opinion-on-preliminary-draft-law-amending-the-act-of-3-december-2017-establishing-the-data-protection-authority.pdf>

<sup>3</sup> CJEU Case C-518/07 – judgement of 9 March 2010 (Commission v. Germany), CJEU Case C- 614/10 – Judgement of 16 October 2012 (Commission v. Austria), CJEU Case C-288/12 – Judgement of 8 April 2014 (Commission v. Hungary).

<sup>4</sup> Opinion 1/15 of the Court of 26 July 2017, para 229, 230 and 232.

<sup>5</sup> See CJEU Case C-518/07 – judgement of 9 March 2010 (Commission v. Germany), para. 36, CJEU Case C- 614/10 – Judgement of 16 October 2012 (Commission v. Austria), para. 51 and CJEU Case C-288/12 – Judgement of 8 April 2014 (Commission v. Hungary), paras. 54, 55 and 60.

<sup>6</sup> This is without prejudice to the assessment made by the European Commission in the infringement procedure against Belgium concerning the appointment of two external members of the GBA/APD, for which the situation is now resolved.

fulfils the conditions required for the performance of the duties.” The EDPB also questions how the various proposals for **increased parliamentary oversight** relate to the requirement to “remain free from external influence” (Article 52(2) GDPR). Lastly, the EDPB recognizes that the proposal to make obligatory use of a **shared service centre** may conflict with Article 52(5) GDPR, as quoted above.

As you are well aware, independent supervision is the cornerstone of effective enforcement. This holds especially true in a system like the GDPR, which is dependent on effective cooperation between equal counterparts. Due to the impact that the draft law may have on the functioning of the GBA/APD and the fact that the draft law is already at an advanced stage at national level, the EDPB considers it important to draw your attention to these developments.

Last, but not least, the EDPB emphasizes that the abovementioned developments may be increasingly pressing considering the upcoming expansion of supervisory powers and tasks of both the national data protection authorities and the Board itself, in view of the adoption of a number of acts in the digital area that are designed to build on the GDPR.<sup>7</sup>

The EDPB remains committed to ensure a full and consistent implementation of the GDPR throughout the EEA and, to that end, facilitates the effective cooperation between its Members and their bilateral and multilateral exchanges of information and best practices, which relies on the authorities’ abilities to act independently and in full capacity.

Yours sincerely,



Aleid Wolfsen

---

<sup>7</sup> Regulation on Privacy and Electronic Communications, Artificial Intelligence Act, Data Governance Act.

# Letters



Sophie in't Veld

MEP European Parliament  
Rue Wiertz 60  
B-1047 Brussels  
Belgium

Brussels, 28 July 2022

Ref: OUT2022-0060

Dear Ms in't Veld,

On behalf of the EDPB, I would like to thank you for the questions you raised in your letter of 28 April 2022 on the PNR Directive, more specifically on the statistical information held by the national supervisory authorities (SAs) and the EDPB on the implementation in the EU Member States, as well as their involvement in the proceedings before the Court of Justice of the European Union (CJEU).

The EDPB considers statistics to be a useful tool – amongst others – to assess the fundamental legal requirements of necessity and proportionality. I would like to assure you that the SAs have been following not only the legislative process in the Member States but also the implementation process very closely. As to the referral by the Belgian Constitutional Court to the CJEU on PNR data, the EDPB has not taken part in the proceedings. However, one of the EDPB members, namely the EDPS, was invited and participated in the hearing.

In the meantime, as you know, the CJEU published its judgment in the case C-817/19 on 21 June 2022. In essence, while leaving the validity of the Directive unaffected, the Court set out strict limitations and required that the powers provided for by that Directive are interpreted restrictively. To name a few of the key findings, the CJEU set up substantial limitations for the collection of PNR data from intra-EU flights and the retention of PNR data. The CJEU also provided guidance for the automated processing of PNR data.

The CJEU has handed down an extremely important decision, which the EDPB is still in the process of analysing. Given the fact that the judgment touches upon some of the key elements of the Directive, it raises also many questions on how all Member States of the European Union, and not only Belgium, have transposed and implemented the Directive. At this stage of the analysis, it seems Member States would have to contemplate substantial amendments of their national law and practice on the processing of PNR data in order to fully follow the CJEU's interpretation.

The SAs assembled in the EDPB are committed to do their part in ensuring that Member States comply with EU law as interpreted by the CJEU.

Yours sincerely,



Ventsislav Karadjov  
Vice-Chair of the EDPB

**Anu Talus**  
Chair of the European Data Protection Board

Emily O'Reilly  
European Ombudsman  
1 avenue du President Robert Schuman  
F-67001 Strasbourg Cedex  
France

Brussels, 28 June 2023

*by e-mail only*  
Ref: 2023-0045

***EDPB Response to the European Ombudsman's recommendation regarding case 201/2022/JK***

Dear Ms O'Reilly,

The EDPB is grateful for your letter of 29 March 2023 enclosing your recommendation on case 201/2022/JK (the “**Recommendation**”), including the confidential annex providing a more detailed assessment on the nature and content of the preparatory documents. The EDPB thanks you for your Recommendation.

As we have noted in our previous correspondence, the EDPB values transparency and is committed to open decision-making and good administration. The EDPB takes a finding of maladministration very seriously and has used this opportunity to review this complaint. Your Recommendation was discussed during the Plenary meetings of the 24-25 May and 20 June 2023.

The EDPB fully supports providing the broadest possible access to the documents at issue, in compliance with Regulation (EC) No 1049/2001 and agrees with your Recommendation. The Court of Justice of the European Union (CJEU) has yet to deliberate and confirm in case law some of the matters in scope of this complaint. In the meantime and in the spirit of transparency and cooperation, the EDPB has endeavoured to achieve your proposed balanced solution. The EDPB agrees to disclose draft versions of documents in scope of the complaint, including with tracked changes, and agrees with your proposal to anonymise such documents so that they are unable to attribute views to a specific author.

The EDPB is pleased to provide you with our opinion in response to your Recommendation. In this opinion, the EDPB has presented the decision taken by the Plenary regarding the different categories of documents, before providing a detailed response to your assessment. We of course remain at your disposal should you wish to engage on these matters bilaterally.

## 1. The EDPB's position regarding the disclosure for each category of documents, following the Ombudsman's Recommendation

Following a reassessment of all the documents in scope of your Recommendation, the EDPB members have discussed this matter during its recent Plenaries of 24 May and 20 June 2023. Consequently, the EDPB has decided to revise its confirmatory decision regarding the disclosure of these documents, in order to grant the widest possible access to them, and fully comply with your Recommendation. The revised EDPB position is set out below, for each category of documents subject to your Recommendation.

### 1.1. Draft versions of EDPB Statement 04/2021<sup>1</sup>

In its confirmatory decision, the EDPB has denied access to 19 draft versions<sup>2</sup> subject to your Recommendation. After a re-assessment of these documents, and taking into consideration your Recommendation, the EDPB has decided to:

- **Fully disclose 18 of these drafts<sup>3</sup>.**
- **Partially disclose the remaining draft<sup>4</sup>. This document will be disclosed in an anonymised form.** The internal comments will not be disclosed because the EDPB considers that redacting the reference to the supervisory authorities ("SAs") which made the comments is not sufficient to ensure the document is anonymised. The EDPB has therefore decided that the contents of these internal comments shall remain confidential, and that the exception of Article 4(3) 2<sup>nd</sup> paragraph of Regulation (EC) No 1049/2001 is applicable in this case. The EDPB is committed to ensuring transparency of its decision-making process, and considers that this is achieved by granting access to the track changes in the document. The EDPB has provided its detailed reasoning on this matter below under Section 2.

### 1.2. Draft versions of the EDPB response to MEP in't Veld<sup>5</sup>

In its confirmatory decision, the EDPB has denied access to 8 draft versions<sup>6</sup> subject to your Recommendation. After a re-assessment of these documents, and taking into consideration your Recommendation, the EDPB has decided to:

---

<sup>1</sup> EDPB Statement 04/2021 on international agreements including transfers, adopted on 13 April 2021. Available at [https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-042021-international-agreements-including\\_en](https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-042021-international-agreements-including_en).

<sup>2</sup> Documents 1, 2, 3, 5, 6, 7, 8, 9, 10, 11, 12, 22, 23, 24, 25, 26, 27, 29, 30.

<sup>3</sup> Documents 1, 2, 3, 5, 6, 7, 8, 9, 10, 11, 12, 22, 23, 24, 25, 27, 29, 30. Please note that documents 8 and 22 are duplicates.

<sup>4</sup> Documents 26.

<sup>5</sup> EDPB response to MEP Sophie in't Veld regarding EDPB Statement 04/2021 on international agreements including transfers, adopted on 7 July 2021. Available at [https://edpb.europa.eu/system/files/2021-07/edpb\\_letter\\_out2021-0119\\_intveld\\_igas.pdf](https://edpb.europa.eu/system/files/2021-07/edpb_letter_out2021-0119_intveld_igas.pdf).

<sup>6</sup> Documents 32, 33, 34, 35, 36, 37, 40, 102.

- **Fully disclose 4 of these drafts<sup>7</sup>.**
- **Partially disclose the 4 remaining drafts<sup>8</sup>. These document will be disclosed in an anonymised form.** The internal comments will not be disclosed because the EDPB considers that redacting the reference to the supervisory authority which made the comment is not sufficient to ensure the documents are anonymised. The EDPB has therefore decided that the contents of these internal comments shall remain confidential, and that the exception of Article 4(3) 2<sup>nd</sup> paragraph of Regulation (EC) No 1049/2001 is applicable in this case. The EDPB is committed to ensuring transparency of its decision-making process, and considers that this is achieved by granting access to the track changes in the documents. The EDPB has provided its detailed reasoning on this matter below under Section 2.

### 1.3. Draft versions of EDPB Guidelines 2/2020<sup>9</sup>

In its confirmatory decision, the EDPB has denied access to 41 draft versions<sup>10</sup> subject to your Recommendation. After re-assessment of these documents, and taking into consideration your Recommendation, the EDPB decided to:

- **Fully disclose 9 of these drafts<sup>11</sup>.**
- **Partially disclose the 32 remaining drafts<sup>12</sup>. The documents will be disclosed in an anonymised form.** The EDPB has decided that some comments in one of the documents<sup>13</sup> may be disclosed, as their contents would not allow the author to be identified, given their general nature. The other internal comments in that document, as well as in the remaining documents, will not be disclosed because the EDPB considers that redacting the reference to the supervisory authority which made the comment is not sufficient to ensure the documents are anonymised. The EDPB has therefore decided that the contents of these internal comments shall remain confidential, and that the exception of Article 4(3)2<sup>nd</sup> paragraph of Regulation (EC) No 1049/2001 is applicable in this case. The EDPB is committed to ensuring transparency of its decision-making process, and considers that this is achieved by granting access to the track changes in the documents. The EDPB has provided its detailed reasoning on this matter below under Section 2.

---

<sup>7</sup> Documents 32, 33, 36, 37. Please note that documents 34 and 35 are duplicates, as well as documents 36 and 37.

<sup>8</sup> Documents 34, 35, 40, 102.

<sup>9</sup> Guidelines 2/2020 on Articles 46(2)(a) and 46(3)(b) of Regulation for transfers of personal data between EEA and non-EEA public authorities and bodies, version 2.0 adopted on 15 December 2020. Available at [https://edpb.europa.eu/our-work-tools/our-documents/guidelines-guidelines-22020-articles-46-2-and-46-3-b-regulation\\_en](https://edpb.europa.eu/our-work-tools/our-documents/guidelines-guidelines-22020-articles-46-2-and-46-3-b-regulation_en).

<sup>10</sup> Documents 45, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 77, 78, 80, 83, 85, 86, 88, 89, 93, 94, 96, 97.

<sup>11</sup> Documents 45, 52, 53, 55, 56, 77, 93, 96, 97

<sup>12</sup> Documents 47, 48, 49, 50, 51, 54, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 78, 80, 83, 85, 86, 88, 89, 94.

<sup>13</sup> Document 47.

## 2. EDPB Response to the Ombudsman's assessment

### 2.1. EDPB reliance on Article 4(3) of Regulation (EC) No 1049/2001

#### 2.1.1 *The risks to the independence of the EDPB and its members*

With regard to the documents partially disclosed, the EDPB considers that the exception under Article 4(3) 2<sup>nd</sup> paragraph of Regulation (EC) No 1049/2001 applies. In the following lines, the EDPB provides detailed arguments in order to explain, in the most precise way possible, its reliance on that exception and the specific and actual risks that disclosure would cause to its decision-making process.

The EDPB fully agrees with and is committed to ensuring transparency of its decision-making process, in line with Articles 1 and 10 TEU and Article 15 TFEU. The EDPB concurs with the Ombudsman in that the principle of transparency applies to all documents held by EU institutions, bodies and agencies, as it “guarantees that the administration enjoys greater legitimacy and is more effective and more accountable to the citizen”<sup>14</sup>. The EDPB also acknowledges that such principle applies regardless of whether the documents form part of the EU’s legislative process<sup>15</sup>.

The EDPB underlines that, in cases where documents are part of the EU’s legislative process, the principle of transparency requires a wider access to the documents, which “should be made directly accessible to the greatest possible extent”<sup>16</sup>. The CJEU has emphasised this in consistent case law, where it recognised the importance of involving citizens in the decision-making process in the context of the legislative process by providing them with timely access to the information<sup>17</sup>. The EDPB highlights that the case law referred to in paragraph 24 of your Recommendation becomes relevant in the context of the legislative process. Indeed, both judgements quoted refer to final versions of internal documents used in the context of a legislative decision-making process<sup>18</sup>. On the contrary, the EDPB is a body with no legislative powers and the documents within the scope of your Recommendation are not final, but rather drafts containing track changes and internal comments made at staff level. Therefore, the findings made by the CJEU in T-144/05 and T-540/15 are not applicable *mutatis mutandis* to the case at hand. This being said, and keeping in mind the Recommendation and the EDPB’s pursue of transparency, the EDPB decided to revisit its approach and disclose all the draft versions of Statement 04/2021, Guidelines 2/2020 and the reply to an MEP, only redacting some of the internal comments made at staff level, in line with your proposal to anonymise the documents. By disclosing these documents, the EDPB believes that it provides the

---

<sup>14</sup> The Recommendation, paragraph 20 and Regulation (EC) 1049/2001, recital 2.

<sup>15</sup> The Recommendation, paragraph 20.

<sup>16</sup> Recital 6 of Regulation (EC) No 1049/2001.

<sup>17</sup> Judgment of 4 September 2018, *ClientEarth v Commission*, [C-57/16 P](#), EU:C:2018:660, paragraph 84 and the case law cited therein.

<sup>18</sup> Judgment of 18 December 2008, *Pablo Muñiz v Commission*, [T-144/05](#), EU:T:2008:596, is about meeting minutes (paragraph 77); and judgment of 22 March 2018, *Emilio de Capitani v European Parliament*, [T-540/15](#), EU:T:2018:167, relates to multi-column tables used during the legislative decision-making process (paragraphs 1, 3-4).

applicant with a clear overview of its decision-making process regarding the specific files, without it being necessary to disclose internal comments made by staff members to achieve this goal.

In this respect, the EDPB wishes to reiterate that disclosure of internal comments containing views and opinions of staff members is not afforded since it could lead to the re-identification of the authors or, at the very least, the party(ies). This risk is not purely hypothetical but real, foreseeable and in fact, based on a previous recent experience: in the context of the Ombudsman Decision in case 386/2021/AMF, disclosure of internal comments where only the authors were anonymised did not prevent the attribution of views to specific parties<sup>19</sup>. This will affect the EDPB's decision-making process as it can be used in an attempt to discredit the EDPB and/or some of its members and/or exert pressure over them. This is especially the case if we take into account the role of the EDPB members at national level as the competent supervisory authorities ("SAs") to ensure compliance with national and EU data protection rules, including the supervision of the Member States' compliance with their obligations. Given the fact that the redacted comments portray opinions and views of national authorities - at staff level - with regard to documents addressing data protection compliance in the field of international agreements and administrative arrangements between public bodies, it is particularly important to ensure that SAs are able to fulfil their tasks in an independent manner and without being subject to any external pressure<sup>20</sup>, including from Member States' governments. Should the internal comments at issue be disclosed, the EDPB considers that there is a reasonably foreseeable risk that Member States' governments attempt to exercise pressure on their competent SA, especially considering that Statement 04/2021 invited Member States to assess and review their international agreements involving international transfers in light of the EU data protection framework, and the SAs' role in supervising compliance with data protection rules.

### **2.1.2 The risks to the EDPB's mission and the decision-making process**

The EDPB also wishes to underline its task of ensuring the consistent application of the GDPR and the LED<sup>21</sup>. In order to achieve such mission, it is essential that the EDPB speaks with one voice in accordance with its guiding principles of collegiality, inclusiveness and cooperation<sup>22</sup>. In this respect, the EDPB understands the added value of the draft documents for stakeholders in order to understand the process leading to the adoption of the final documents. The different draft versions are a result of the discussions, cooperation and agreements of the EDPB members during the decision-making process and reflect the different stages which the documents underwent. In this respect, the

---

<sup>19</sup> Please see for instance of the public allegations by some stakeholders following disclosure of draft guidelines 2/2019 following the Ombudsman Decision in case 386/2021/AMF: noyb, *noyb's Second "Advent Reading": How the Irish DPC tried to lobby Facebook's "GDPR bypass" into European Guidelines* (available at <https://noyb.eu/en/second-noyb-advent-reading-facebookdpc-documents>); Politico, '*Contrary to everything we believe in': Irish data watchdog lobbied for business-friendly GDPR* (available at <https://www.politico.eu/article/irish-data-protection-commission-gdpr-lobby-business-friendly-general-data-protection-regulation/>).

<sup>20</sup> Article 39 TEU; Article 16(2) TFEU; Article 8(3) EU Charter; Article 52 Regulation 2016/679 ("GDPR"); Article 42 Directive 2016/680 ("LED").

<sup>21</sup> Article 70 GDPR and Article 51(1)(b) LED. See also Article 2 of the EDPB's Rules of Procedure (available at [https://edpb.europa.eu/our-work-tools/our-documents/rules-procedure/rules-procedure-version-8\\_en](https://edpb.europa.eu/our-work-tools/our-documents/rules-procedure/rules-procedure-version-8_en)).

<sup>22</sup> Article 3 EDPB Rules of Procedure.

documents that the EDPB proposes to disclose already provide the public with a clear understanding of how the EDPB interpreted the GDPR in the given cases<sup>23</sup>, without jeopardising the EDPB's mission to speak with one voice.

By contrast, the EDPB is of the view that its role will be undermined in the event that internal deliberations are made public. Indeed, the redacted comments contain opinions for internal use as part of deliberations and preliminary consultations within the EDPB whose disclosure would undermine the decision-making process of the EDPB<sup>24</sup>. Firstly, the EDPB underlines that the internal comments at hand were made during the drafting stage at staff level and do not necessarily reflect the official position of the concerned EDPB members. If staff members fear that internal comments expressed during deliberations may be made public, this could lead to the censoring of their own views and opinions<sup>25</sup>. In this regard, even if the internal comments were anonymised by redacting only the name of the individuals and/or of their SA, there is still a risk of re-identifying the SA of the staff member and, therefore, the concrete author of the comment could also be identified<sup>26</sup>. This is a real, foreseeable and tangible risk which some EDPB members have already shared concerns about. This will undoubtedly have a very significant negative impact on the EDPB's deliberations during its decision-making processes. In this respect, the EDPB wishes to emphasise once again its working methods, whereby the EDPB members play an essential role in feeding the work of the EDPB. This is particularly the case in relation to guidelines, statements and other guidance, where the rapporteurs are usually SAs. In addition, in the context of the discussions in the dedicated expert subgroups, the EDPB members have a prominent role in providing written and oral comments, discussing options and reaching compromises. This is clearly reflected by the several draft versions of the statement, guidelines and letter within the scope of this case. Therefore, should some EDPB members censor sharing their views in preparatory work that is essential in the proper running of the EDPB, the risk that the EDPB is not able to fully achieve its tasks in the future, at least when it comes to drafting and adopting guidance, is reasonably foreseeable and not merely hypothetical<sup>27</sup>.

Considering the above, and with the aim of fully complying with your Recommendation of providing the broadest possible access to the documents in an anonymised format, the EDPB decided to disclose all the drafts at issue, including those with track changes, and only redact the information whose disclosure was essential to protect the fulfilment of its mission and its decision-making process.

---

<sup>23</sup> In relation to the views expressed by the Ombudsman in paragraph 29 of the Recommendation.

<sup>24</sup> Judgment of 21 July 2011, *Sweden v MyTravel and Commission*, [C-506/08 P](#), EU:C:2011:496 paragraph 78; and judgment of 22 May 2012, *Internationaler Hilfsfonds v Commission*, [T-300/10](#), EU:T:2012:247, paragraph 131.

<sup>25</sup> Judgment of 15 September 2016, *Philip Morris v Commission*, [T-18/15](#), EU:T:2016:487, paragraph 87: "[...] *The possibility of expressing views independently within an institution helps to encourage internal discussions with a view to improving the functioning of that institution and contributing to the smooth running of the decision-making process*" (emphasis added).

<sup>26</sup> For example, the use of specific language or formulations can give an indication of the geographical location or mother tongue of the author of the comment, which could be an element to identify either the SA, or the author or both. See section 2.1.3 below.

<sup>27</sup> Judgment of 22 May 2012, *Internationaler Hilfsfonds v Commission*, [T-300/10](#), EU:T:2012:247, paragraph 91 and 92 and case law cited therein.

Finally, the EDPB wishes to clarify its previous references to the need to preserve its independence<sup>28</sup>. The independence of the EDPB and its members is an essential element to enable the EDPB's task of ensuring the consistent application of the GDPR<sup>29</sup> and encouraging the consistent application of the LED<sup>30</sup>, as well as the SAs' task of monitoring the application of the GDPR<sup>31</sup> and of the provisions adopted pursuant to the LED<sup>32</sup>. In line with this, the EDPB Rules of Procedure establish the rules on confidentiality of the discussions in several situations, including when the EDPB decides so given the nature of the topic<sup>33</sup>. The EDPB fully agrees with the Ombudsman in that internal rules of procedure do not take legal precedence over a Regulation, and reassures that this was never the understanding nor intention of the EDPB. On the contrary, the EDPB fully abides by the obligation stemming from Regulation (EC) No 1049/2001 and the case law to demonstrate that the risks posed by the disclosure of the internal comments at hand are real, foreseeable and not purely hypothetical, in addition to demonstrating that there is no overriding public interest<sup>34</sup>. The independence of the EDPB and its confidentiality rules are mere elements stemming from the GDPR and the EDPB's Rules of Procedure which substantiate the EDPB's views that its decision-making process may be undermined by the disclosure of these internal comments, given the negative effect that it may have in the independence of the EDPB and its members. Thus, as explained above, the EDPB took these aspects into consideration when determining whether disclosure should be rejected on the basis of Article 4(3) of Regulation (EC) No 1049/2001.

### ***2.1.3 The lack of an overriding public interest in disclosure of the comments***

As required by Article 4(3) Regulation (EC) No 1049/2001, the assessment of the applicability of an exception consists of balancing the opposing interests in a given situation, which outcome shall favour the interest prevailing in the particular case<sup>35</sup>.

We note that your comments on this aspect are focussing on the draft versions of Guidelines 2/2020, hence we understand them as not questioning the EDPB's assessment of whether an overriding interest was prevailing for the application of exceptions to the draft versions of Statement 04/2021 and the reply to MEP in't Veld.

Regarding Guidelines 2/2020, the EDPB wishes to reassure the Ombudsman<sup>36</sup> that this balancing exercise has been duly performed in this particular case. Whilst the CJEU keeps exclusive jurisdiction over the authoritative interpretation of EU law<sup>37</sup>, we thank you for the consideration you attach to

---

<sup>28</sup> In relation to the views expressed by the Ombudsman in paragraphs 35-36 of the Recommendation.

<sup>29</sup> Articles 69-71 GDPR.

<sup>30</sup> Article 51(1)b) LED.

<sup>31</sup> Articles 51, 52 and 57 GDPR.

<sup>32</sup> Articles 41, 42 and 46 LED.

<sup>33</sup> Article 33 of the EDPB's Rules of Procedure.

<sup>34</sup> See section 2.1.3.

<sup>35</sup> Judgment of 27 November 2018, *VG v Commission*, joined cases T-314/16 and T-435/16, EU:T:2018:841, paragraph 60 and case-law cited.

<sup>36</sup> In relation to the views expressed in paragraph 30 of the Recommendation.

<sup>37</sup> Judgment of 6 February 2020, *Compañía de Tranvías de la Coruña v Commission*, T-485/18, EU:T:2020:35, paragraph 83 and case-law cited.

guidelines adopted by the EDPB. They are indeed a valuable tool contributing to ensuring the consistent application of the GDPR - the EDPB's main task<sup>38</sup>.

Concerning the drafts of Guidelines 2/2020 that do not contain any track changes or internal comments made by staff, the EDPB acknowledges that the interest of stakeholders in understanding how the EDPB's decision-making process relating to these Guidelines 2/2020 worked, prevails. The same applies to the draft versions of these Guidelines that contain track changes (without internal comments). This is why we agree to fully disclose these documents with the complainant.

As per the draft versions of Guidelines 2/2020 that contain track changes and internal comments made by staff, we also acknowledge the overriding public interest in accessing such documents with their track changes, for the same reasons as explained above. The EDPB considers that such disclosure is sufficient to enable people understanding how the EDPB's decision-making process worked, without any need to access the internal comments made by staff, which are redacted to anonymise their authors, as recommended by the Ombudsman.

On that aspect, we underline that, like the Ombudsman<sup>39</sup>, the EDPB has no knowledge of publicly known dissenting views on the subject-matter addressed by Guidelines 2/2020, contrary to the situation arisen for Guidelines 2/2019<sup>40</sup>. This could however change in the future. Besides, as explained above, simply hiding the name of the authors who made internal comments in a document is not an efficient method to anonymise such comments. It is true that they could appear anonymous at first sight<sup>41</sup>, but the application of one or more factors specific to some members of the EDPB could re-identify the authors of these internal comments.

Furthermore, the EDPB can only agree with the Ombudsman<sup>42</sup> that personal data are important for citizens and businesses. This is precisely why the decision-making process of the EDPB should be protected, where necessary, to ensure consistent application of the data protection legislation throughout the EEA. Therefore, the EDPB considers that the public interest of data protection overrides, in these specific circumstances, the public interest in disclosing the internal comments made by staff.

For the sake of clarity, the EDPB indicates that its position above also applies to the internal comments made by staff in the draft versions of Statement 04/2021 and of the reply to MEP in't Veld.

### 3. Concluding remarks

In light of the above, we consider that the EDPB has sufficiently demonstrated a specific and actual risk to its decision-making, and the absence of an overriding public interest in disclosure of the internal comments.

---

<sup>38</sup> Article 70 GDPR.

<sup>39</sup> Paragraph 29 of the Recommendation.

<sup>40</sup> In relation to the reference included in footnote 16, under paragraph 30 of the Recommendation.

<sup>41</sup> Judgment of 19 March 2013, *In 't Veld v Commission*, EU:T:2013:135, paragraph 126.

<sup>42</sup> Paragraph 31 of the Recommendation.



European Data Protection Board

To conclude, we would like to reiterate our intention to proactively apply the same approach as presented above, for future requests concerning revised versions of documents, where relevant, taking always into account the specificities of the request(s) assessed. We stand ready to review these arrangements regularly to ensure they remain fit for purpose.

As requested, we are enclosing a translation into French of this reply. Please note that in order to provide this reply within the deadline, only a machine translation could be provided. We trust that you will appreciate this sincere effort and the action, under our existing constraints. Considering that the language of the complaint in case 201/2022 was English, please let us know should a formal translation be required.

We would like to conclude by reassuring you again that the EDPB takes transparency matters very seriously, and will continue to do so in the future.

Yours sincerely,

Anu Talus

Chair of the EDPB

Roberta Metsola  
Member of the European Parliament

Andrzej Halicki  
Member of the European Parliament

By email only

Ref: OUT2020-0041

Dear Ms. Metsola, Dear Mr. Halicki,

Thank you for your letters and for bringing this issue to the attention of the European Data Protection Board (EDPB). The fact that data of Polish citizens was sent from the national PESEL (personal identification) database to the Polish Post by one of the ministries appears to require special attention. Due to the upcoming elections, the EDPB decided to handle this matter urgently.

Taking into consideration that elections constitute the cornerstone of every democratic society, I would like to reassure you that the EDPB dedicates special attention to the issue of processing of personal data for election purposes, as we already demonstrated during the preparation for the 2019 European Parliament elections.<sup>1</sup>

With respect to supervision over personal data processing, I would like to stress that the EDPB does not have the same competences, tasks and powers as national supervisory authorities. The assessment of alleged infringements of the GDPR, in the first instance, falls within the competence of the responsible and independent national supervisory authority.

Data protection supervisory authorities are responsible for monitoring and, if necessary, enforcing the application of data protection principles in the context of elections and political campaigns, such as lawfulness, transparency, purpose limitation, proportionality and security, as well as the exercise of data subject rights. A judicial remedy should also always be available in accordance with articles 78 and 79 GDPR.

The EDPB underlines that according to the GDPR, personal data, such as names and addresses, and national identification numbers (such as the Polish PESEL ID), must be processed lawfully, fairly and in a transparent manner, for specified purposes only. Public authorities may disclose information about individuals included in electoral lists when this is specifically authorised by Member State law. I would like to underline that the disclosure of personal data – from one entity to another – always requires a legal basis in accordance with EU data protection laws. As previously indicated in the EDPB statement 02/2019 on political campaigns, political parties and candidates – but also public authorities, particularly those responsible for public registers – must stand ready to demonstrate how they have

<sup>1</sup> Please see the EDPB Statement 2/2019 on the use of personal data in the course of political campaigns [https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections\\_en.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf)

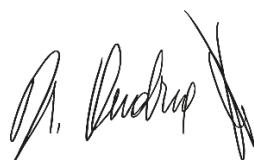
complied with data protection principles, especially the principles of lawfulness, fairness and transparency.

The EDPB would also like to underline that, where elections are conducted by the collection of postal votes, it is the responsibility of the state to ensure that specific safeguards are in place to maintain the secrecy and integrity of the personal data concerning political opinions.

In addition, I would like to stress that in the context of data processing, there is a specific responsibility on public authorities, in particular those responsible for public registers. The EDPB encourages these data controllers to lead by example and process personal data in a manner, which is transparent and leaves no doubt regarding, among others, the legal basis for the processing operations, including disclosure of data.

We wish to reassure you that the EDPB will continue to pay special attention to the developments of personal data processing in connection to democratic elections and remain ready to support all members of the EDPB, including the Polish Supervisory Authority, in such matters.

Yours sincerely,



Andrea Jelinek



European Data Protection Board

## Anu Talus

Chair of the European Data Protection Board

Mr. Viola  
European Commission  
Rue de la Loi 51,  
1040 Brussels  
Belgium

Mr. Guersent  
European Commission  
Place Madou 1  
1210 Brussels  
Belgium

Brussels, 18 July 2024

**Subject: Guidelines on the interplay between DMA and GDPR**

Dear Mr. Viola, dear Mr. Guersent,

Thank you for your letter concerning the EDPB's ongoing work on Guidelines on the interplay between the Digital Markets Act (DMA) and the General Data Protection Regulation (GDPR). I would also like to take this opportunity to thank you for the constructive exchanges in the context of the DMA High Level Group (DMA HLG) and in the context of the EDPB Task Force on Competition & Consumer Law. I consider these fruitful exchanges instrumental to promoting cross-regulatory consistency.

The EDPB's commitment to foster cross-regulatory consistency is an integral part of the EDPB Strategy 2024–2027. Developing guidance on the interplay between the application of the GDPR and other EU legal acts, such as the DMA, is one of the key actions listed in the EDPB strategy. Securing cooperation with other regulatory authorities on matters with an impact on data protection, including authorities competent under other legal acts, such as the DMA, is another key action.

The EDPB initiated work on Guidelines on the interplay between the DMA and GDPR to offer guidance on how to interpret and apply the GDPR when gatekeepers process personal data in the contexts covered by the DMA<sup>1</sup>. The DMA confirms that it applies without prejudice to the rules contained in the GDPR, and that the processing of personal data by gatekeepers therefore remains subject to the supervision of independent data protection authorities. In this regard, the EDPB has full competence to issue guidelines on any matter concerning the application of the GDPR and our work on the guidelines does not seek to impinge on the sole competence of the Commission to interpret and apply the DMA as such.

This notwithstanding, I appreciate your suggestion and willingness to discuss and explore the appropriate shape and form of a project aimed at providing coherent guidance on the intersection of the DMA and the GDPR, reflecting jointly the respective views of the competent regulators.

---

<sup>1</sup> Given the transversal nature of the GDPR, the EDPB has already on several occasions issued guidance on the interplay between the GDPR and other instruments of EU law (such as the PSD2 and the ePrivacy Directive).



European Data Protection Board

A joint deliverable between the EDPB and the European Commission could indeed be an important opportunity to foster legal certainty, as well as cross-regulatory consistency, including in enforcement, and so could provide significant value above-and-beyond that of independently-produced documents.

The EDPB is therefore open to further discuss the parameters and steps towards the preparation of a joint deliverable in an ad-hoc format that would preserve the respective competences, roles and independence of the EDPB and the Commission. I understand that the discussion will take place at a technical level to clarify these matters. Nevertheless, please be reassured that I remain available to discuss the matter further if needed.

Yours sincerely,

Anu Talus

Cc : Ms. Anna Gallego, Director General, DG JUST.



European Data Protection Board

**Anu Talus**

Chair of the European Data Protection Board

Mr Olivier Guersent  
DG COMP  
European Commission

Ms Ana Gallego Torres  
DG JUST  
European Commission

Brussels, 07 October 2024

*Via Ares*

Your ref: COMP A4 /MK

**Subject: EDPB work on the interplay between EU data protection and competition law**

Dear Mr Guersent and Ms Gallego Torres,

Thank you for your letter of 21 August on the EDPB's ongoing work on a position paper regarding the interplay between EU data protection and competition law.

The position paper aims to outline how the objectives and concepts of data protection and competition law relate to each other, and how cooperation between competition authorities and data protection authorities could be further developed. It also aims to explore the interplay with, and harness the synergies between, EU data protection and competition law, focusing, at a high level, on the role of competition and market considerations in data protection practices. I would take this opportunity to clarify that the position paper is intended to be a public statement. In these contexts, I would like to reassure you that the EDPB's sole intention is to focus on issues of data protection and cooperation, and so tackle these issues from within its competences, and that the EDPB hopes to take full advantage of the Commission's expertise as part of our regular exchanges at Taskforce level.

The EDPB very much welcomes the continued contributions from, and collaboration with, the Commission as this work continues to progress in the Taskforce. I would, further, like to reiterate our support for cooperation regarding the interplay between data protection and competition in the wider sense, such as in our preparations for joint guidance on the interplay between the GDPR and the DMA.

I hope that this helps to assuage your concerns on this matter.

Yours sincerely,

Anu Talus

European Data Protection Board  
Rue Wiertz, 60  
1047 Brussels