



## A new level of cooperation between European regulators

The European Data Protection Board (EDPB), a new independent EU body, brings together all supervisory authorities in the EEA, as well as the European Data Protection Supervisor. The EDPB contributes to the consistent application of the GDPR by:

- providing general guidance;
- promoting cooperation and the exchange of information between the EEA SAs;
- ensuring consistency of the enforcement by the EEA SAs;
- advising the European Commission on any issue related to data protection.

## Stronger enforcement of your data protection rights

Enforcement lies with the EEA SAs, who saw their enforcement powers significantly increased with the entry into application of the GDPR. They are now able to impose fines up to 10 or 20 million EUR or 2 to 4% of an organisation's worth, depending on the seriousness of the infringement.

### Do you think your data protection rights have been violated?

You can contact the organisation holding your data, contact your national supervisory authority, or go to a national court. Supervisory authorities can conduct investigations and impose sanctions where necessary. You can find the contact details for all EEA supervisory authorities on the EDPB website.

### Do you think your data has been lost or stolen?

The GDPR puts in place clear procedures in case of a data breach. If a data breach poses a risk, companies and organisations holding your data have to inform the relevant data protection authority within 72 hours or without undue further delay. If the leak poses a high risk to you, then you must also be informed personally.

Editor: Secretariat of the European Data Protection Board, Rue Montoyer 30, 1047 Brussels.



# GDPR and your rights

## Data protection, a fundamental right for every EU data subject



Internet usage and the amount of data you share every time you go online is at an all-time high and will continue to rise. Whether through online shopping, social media or a simple search engine query, you are leaving information about yourself behind. This comes with risks, from your data being sold to the highest bidder without your knowledge and profiling, to online abuse and identity theft.

The General Data Protection Regulation (GDPR), which entered into application on 25 May 2018, makes data protection a reality by ensuring a harmonised approach across the EU, Iceland, Liechtenstein and Norway (EEA).

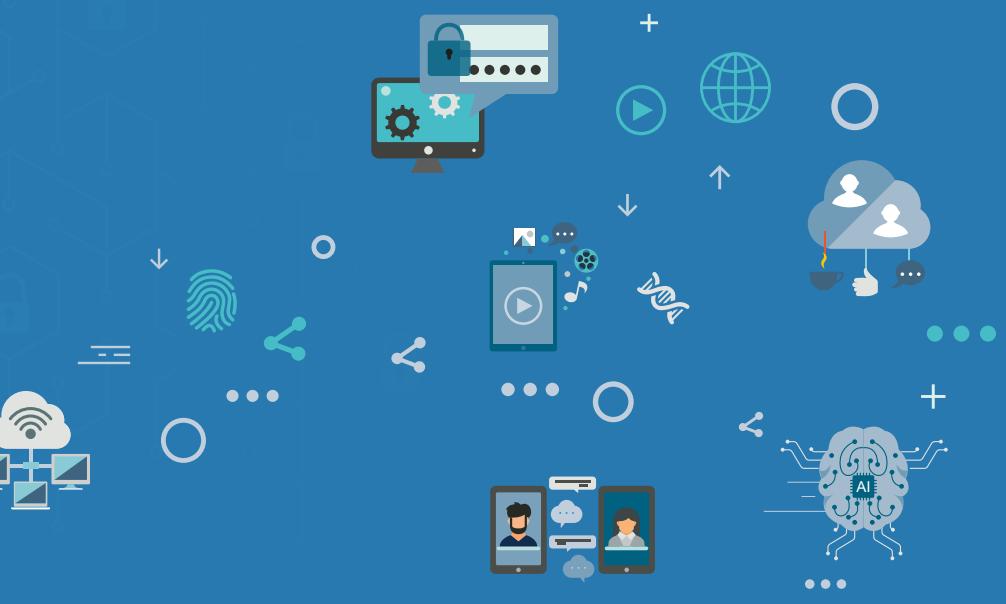
## What changed for you?

**Stronger rules on data protection mean people have more control over their personal data. The new data protection rules give you more control over your personal data and improve your security both online and offline.**

- Clear indication of consent and higher transparency:** When organisations need your consent to process your personal data, they will have to ask you for this and clearly indicate for which purposes your data will be processed.
- Right to receive clear and understandable information:** You have the right to know who is processing your data, what data is being processed and why.
- Right to access your data:** You have the right to request access to the personal data an organisation has about you, free of charge, and to obtain a copy in an accessible format.

- Right to object:** If an organisation is processing your data, you may have the right to object. In some circumstances, such as scientific research, public interest may prevail. You always have the right to object to receiving direct marketing communication.
- Right to correct your data:** If you believe the personal data held on you might be incorrect, incomplete or inaccurate, you have the right to request a correction.
- Right to erasure:** You have the right to ask to delete your personal data, when you no longer want it to be processed, and when there is no legitimate reason to keep it.
- Right to data portability:** When moving from one service provider to another, you have the right to request that your data is returned to you in an easily transmissible format or, if technologically feasible, directly transmitted to your new provider.

*Please note, however, that exceptions to these rights may be foreseen in the GDPR or in national laws.*





European Data Protection Board

**Anu Talus**

Chair of the European Data Protection Board

Lucilla Sioli  
Head of EU AI Office

[REDACTED]  
Artificial Intelligence Office  
CNECT.A.2  
Brussels

Brussels, 6 November 2024

**Subject: Response to the letter on European Data Protection Board (EDPB) statement on the role of data protection authorities (DPAs) in the Artificial Intelligence Act Framework.**

Dear Mrs. Sioli, [REDACTED]

I would like to thank [REDACTED] for his letter of 29 August 2024 (Ares(2024)6134122), sent at the request of President Ursula von der Leyen, regarding the European Data Protection Board's (EDPB) statement on the role of data protection authorities (DPAs) in the Artificial Intelligence Act Framework.

First and foremost, I appreciate your expressed interest in working with the EDPB to ensure a coordinated approach to AI governance. I would also like to reaffirm that the EDPB values the opportunity to engage with the AI Office and the AI Board considering the strong entanglement between the AI Act and data protection law. As highlighted in the EDPB 2024–2027 Strategy, ensuring consistency and cooperation with other regulatory authorities is a strategic priority for the Board, as this is key to promoting the right to data protection in the overall regulatory architecture and contributes to a consistent application of different regulatory frameworks. In that regard, the EDPB has started to work on guidelines on the interplay between the GDPR and the AI Act, on which a discussion with your team would be welcomed.

We therefore support the establishment of appropriate mechanisms to ensure cooperation between the EDPB, the AI Office and the AI Board, also in light of Articles 2(3)(c) and (d), and 6 of the Commission Decision of 24 January 2024 establishing the European Artificial Intelligence Office, C/2024/1459, articles 65(2) and 66(h) of the Artificial Intelligence Act, and article 70(4) of the General Data Protection Regulation.



European Data Protection Board

In this regard, I would like to invite you to the EDPB plenary meeting of 2 or 3 December 2024 in order to discuss this matter. I would also be grateful if you could present information relating to the establishment of the AI office and the AI Board at this meeting, as well as on any other matter that you consider beneficial to our cooperation.

Within this framework, I would like to also draw your attention to the need for taking due account of the requirements laid down in Article 74(8) of the AI Act regarding high-risk AI systems, as stated in the EDPB statement on the role of DPAs in the Artificial Intelligence Act Framework.

In addition, the EDPB is currently working on an Article 64(2) GDPR Opinion on AI models, for which the legal deadline for adoption is on 23 December, and for which an exchange of views with the AI Office would be beneficial.

For this reason, I would like to invite the AI Office to take part in one of the meetings organised at technical level by the EDPB for the preparation of this Opinion on 21 November, 2024. This would be an opportunity to exchange views on this matter. In addition, I welcome the participation of the AI office in the public event that the EDPB organises on 5 November, 2024.

Reciprocally, the EDPB would be pleased to present the opinion it will adopt on AI models during a future meeting of the AI Board, in the first semester 2025.

If you need further assistance, please contact Isabelle Vereecken [REDACTED] Head of EDPB Secretariat) or Gwendal Le Grand [REDACTED] Deputy Head of EDPB Secretariat).

Kind regards,

Anu Talus

# Letters



Florin Dănescu  
Executive President of Romanian association of banks  
4-6 Aleea Negru Voda, district 3  
Bucharest  
Romania

Brussels, 6 April 2021  
Ref: OUT2021-00066

**By e-mail only**

Dear Mr Dănescu,

Let me first of all thank you for your letter of 2 December 2020 to the European Data Protection Board (EDPB) and for the several inputs you have provided.

In your letter, you raise the importance of the interplay between the Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) framework and the General Data Protection Regulation ("GDPR"), particularly in the context of Know Your Customer (KYC) procedures provided for by law.

As you may be aware, the EDPB has recently issued a statement on the protection of personal data processed in relation with the prevention of money laundering and terrorist financing<sup>1</sup>. In this statement we acknowledge the challenging nature of the issue, (also raised in the past by the Article 29 Working Party), in particular in respect of the far-reaching obligations on financial services providers and other obliged entities to identify and know their customers, to monitor transactions undertaken using their services, and to report any suspicious transactions.

The EDPB realises the relevance of the points raised by the Romanian Association of Banks and is grateful for the provided analysis. However, the concrete question raised in your letter appears to refer to a specific cooperation procedure to be developed and applied in Romania only. As this can relate to Romanian national law we suggest you to contact the Romanian Supervisory Authority competent for data protection (Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal), which will be in the best position to advise you on this matter.

---

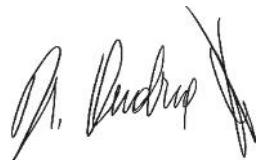
<sup>1</sup> The Statement has been adopted by the Board on the 17th of December 2020 and is available at the following link: [https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_statement\\_20201215\\_aml\\_actionplan\\_en.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_20201215_aml_actionplan_en.pdf)

**Andrea Jelinek**  
Chair of the European Data Protection Board

rue Wiertz, 60  
1047 Brussels

At the same time, I would like to assure you that the Board shall remain concerned about the importance of ensuring the balance between the protection of personal data and the prevention of money laundering and terrorist financing.

Yours sincerely,



Andrea Jelinek

# Guidelines



**Guidelines 03/2022 on  
Deceptive design patterns in social media platform  
interfaces:  
how to recognise and avoid them**

**Version 2.0**

**Adopted on 14 February 2023**

## Version history

Version 2.0	14 February 2023	Adoption of the Guidelines after public consultation
Version 1.0	14 March 2022	Adoption of the Guidelines for public consultation

## EXECUTIVE SUMMARY

These Guidelines offer practical recommendations to social media providers as controllers of social media, designers and users of social media platforms on how to assess and avoid so-called “deceptive design patterns” in social media interfaces that infringe on GDPR requirements. To this end, the EDPB recommends that controllers make use of interdisciplinary teams, consisting, among others, of designers, data protection officers and decision-makers. It is important to note that the list of deceptive design patterns and best practices, as well as the use cases, are not exhaustive. Social media providers remain responsible and accountable for ensuring the GDPR compliance of their platforms.

### Deceptive design patterns in social media platform interfaces

In the context of these Guidelines, “deceptive design patterns” are considered as interfaces and user journeys implemented on social media platforms that attempt to influence users into making unintended, unwilling and potentially harmful decisions, often toward a decision that is against the users’ best interests and in favour of the social media platforms interests, regarding the processing of their personal data. Deceptive design patterns aim to influence users’ behaviour and can hinder their ability to effectively protect their personal data and make conscious choices. Data protection authorities are responsible for sanctioning the use of deceptive design patterns if these breach GDPR requirements. The deceptive design patterns addressed within these Guidelines can be divided into the following categories:

- **Overloading** means users are confronted with an avalanche/large quantity of requests, information, options or possibilities in order to prompt them to share more data or unintentionally allow personal data processing against the expectations of the data subject.  
The following three deceptive design pattern types fall into this category: ***Continuous prompting, Privacy Maze and Too Many Options***
- **Skipping** means designing the interface or user journey in a way that users forget or do not think about all or some of the data protection aspects.  
The following two deceptive design pattern types fall into this category: ***Deceptive Snugness and Look over there***
- **Stirring** affects the choice users would make by appealing to their emotions or using visual nudges.  
The following two deceptive design pattern types fall into this category: ***Emotional Steering and Hidden in plain sight***
- **Obstructing** means hindering or blocking users in their process of becoming informed or managing their data by making the action hard or impossible to achieve.  
The following three deceptive design pattern types fall into this category: ***Dead end, Longer than necessary and Misleading action***

- **Fickle** means the design of the interface is inconsistent and not clear, making it hard for the user to navigate the different data protection control tools and to understand the purpose of the processing.  
The following four deceptive design pattern types fall into this category: ***Lacking hierarchy, Decontextualising, Inconsistent Interface*** and ***Language Discontinuity***
- **Left in the dark** means an interface is designed in a way to hide information or data protection control tools or to leave users unsure of how their data is processed and what kind of control they might have over it regarding the exercise of their rights.  
The following two deceptive design pattern types fall into this category: ***Conflicting information*** and ***Ambiguous wording or information***

### **Relevant GDPR provisions for deceptive design pattern assessments**

Regarding the data protection compliance of user interfaces of online applications within the social media sector, the data protection principles applicable are set out within Article 5 GDPR. The principle of fair processing laid down in Article 5 (1) (a) GDPR serves as a starting point to assess whether a design pattern actually constitutes a “deceptive design pattern”. Further principles playing a role in this assessment are those of transparency, data minimisation and accountability under Article 5 (1) (a), (c) and (2) GDPR, as well as, in some cases, purpose limitation under Article 5 (1) (b) GDPR. In other cases, the legal assessment is also based on conditions of consent under Articles 4 (11) and 7 GDPR or other specific obligations, such as Article 12 GDPR. Evidently, in the context of data subject rights, the third chapter of the GDPR also needs to be taken into account. Finally, the requirements of data protection by design and default under Article 25 GDPR play a vital role, as applying them before launching an interface design would help social media providers avoid deceptive design patterns in the first place.

### **Examples of deceptive design patterns in use cases of the life cycle of a social media account**

The GDPR’s provisions apply to the entire course of personal data processing as part of the operation of social media platforms, i.e. to the entire life cycle of a user account. The EDPB gives concrete examples of deceptive design pattern types for the following different use cases within this life cycle: the sign-up, i.e. registration process; the information use cases concerning the privacy notice, joint controllership and data breach communications; consent and data protection management; exercise of data subject rights during social media use; and, finally, closing a social media account. Connections to GDPR provisions are explained in two ways: firstly, each use case explains in more detail which of the above-mentioned GDPR provisions are particularly relevant to it. Secondly, the paragraphs surrounding the deceptive design pattern examples explain how these infringe on the GDPR.

### **Best practice recommendations**

In addition to the examples of deceptive design patterns, the Guidelines also present best practices at the end of each use case, as well as in Annex II to these Guidelines. These contain specific recommendations for designing user interfaces that facilitate the effective implementation of the GDPR.

### **Checklist of deceptive design pattern categories**

A checklist of deceptive design pattern categories can be found in Annex I to these Guidelines. It provides an overview of the abovementioned categories and the deceptive design pattern types, along with a list of the examples for each pattern that are mentioned in the use cases. Some readers may find it useful to use the checklist as a starting point to discover these Guidelines.

## Table of contents

1	Scope .....	8
2	Principles Applicable – What to keep in mind? .....	11
2.1	Accountability.....	12
2.2	Transparency .....	12
2.3	Data protection by design and default .....	13
3	The life cycle of a social media account: putting the principles into practice.....	15
3.1	Opening a social media account.....	15
	Use case 1: Registering an account .....	15
3.2	Staying informed on social media.....	26
	Use case 2a: A layered privacy notice.....	26
	Use case 2b: Providing information about joint controllership to the data subject, Article 26 (2) GDPR .....	32
	Use case 2c: Communication of a personal data breach to the data subject .....	33
3.3	Staying protected on social media.....	36
	Use case 3a: Managing one's consent while using a social media platform.....	36
	Use case 3b: Managing one's data protection settings .....	43
3.4	Staying right on social media: Data subject rights .....	50
	Use case 4: How to provide proper functions for the exercise of data subject rights .....	50
3.5	So long and farewell: leaving a social media account .....	57
	Use case 5: pausing the account/erasure of all personal data .....	57
4	Annex I: List of deceptive design pattern categories and types .....	65
4.1	Overloading .....	65
4.1.1	Continuous prompting .....	65
4.1.2	Privacy Maze .....	65
4.1.3	Too many options .....	66
4.2	Skipping .....	66
4.2.1	Deceptive snugness.....	66
4.2.2	Look over there.....	66
4.3	Stirring .....	67
4.3.1	Emotional Steering.....	67
4.3.2	Hidden in plain sight.....	67
4.4	Obstructing .....	68
4.4.1	Dead end.....	68
4.4.2	Longer than necessary .....	68

4.4.3	Misleading action .....	68
4.5	Fickle .....	69
4.5.1	Lacking hierarchy .....	69
4.5.2	Decontextualising.....	69
4.5.3	Inconsistent interface .....	69
4.5.4	Language discontinuity .....	70
4.6	Left in the dark.....	70
4.6.1	Conflicting information .....	70
4.6.2	Ambiguous wording or information .....	70
5	Annex II: Best practices .....	73

# The European Data Protection Board

Having regard to Article 70 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>1</sup>

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

## HAS ADOPTED THE FOLLOWING GUIDELINES

### 1 SCOPE

1. The aim of these Guidelines is to provide recommendations and guidance for the design of the interfaces of social media platforms. For the purposes of these Guidelines, social media are understood as online platforms that enable the development of networks and communities of users, among which information and content is shared.<sup>2</sup> The Guidelines can be used either at the conception phase of a user interface, to avoid the implementation of deceptive design patterns<sup>3</sup> from the start, or on an existing service, to evaluate the compliance of its interface. They are aimed at social media providers as controllers of social media, who have the responsibility for the design and operation of social media platforms. In this regard, the Guidelines aim to recall the obligations coming from the GDPR, with special reference to the principles of lawfulness, fairness, transparency, purpose limitation and data minimisation in the design of user-interfaces and content presentation of their web services and apps. The aforementioned principles have to be implemented in a substantial way and, from a technical perspective, they constitute requirements for the design of software and services, including user interfaces. An in-depth study is made on the GDPR’s requirement when applied to user interfaces and content presentation, and it is going to be clarified what should be considered a “deceptive design pattern”, a way of designing and presenting content which substantially violates those requirements, while still pretending to formally comply. These Guidelines are also suitable for increasing the awareness of users regarding their rights, and the risks possibly coming from sharing too many data or sharing their data in an uncontrolled way. These Guidelines also aim to educate users to recognise “deceptive design patterns” (as defined in the following), and how to face them to protect their privacy in a conscious way. As part of the analysis, the life cycle of a social media account was examined on the basis of five use cases: “Opening a social media account” (use case 1), “Staying informed on social media” (use case 2), “Staying protected on social media” (use case 3), “Staying right on social media:

---

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

<sup>2</sup> Definition identical to EDPB Guidelines 08/2020 on Targeting of social media users, para. 1, see footnote 1 there for more detailed description; available at [https://edpb.europa.eu/system/files/2021-04/edpb\\_guidelines\\_082020\\_on\\_the\\_targeting\\_of\\_social\\_media\\_users\\_en.pdf](https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf).

<sup>3</sup> For version 2.0 of these Guidelines, the EDPB is using the more inclusive and descriptive term “deceptive design pattern” instead of “dark pattern”.

- data subject rights” (use case 4) and “So long and farewell: leaving a social media account” (use case 5).
2. In these Guidelines, the term “user interface” corresponds to the means for people to interact with social media platforms. The document focuses on graphical user interfaces (e.g. used for computer and smartphone interfaces), but some of the observations made may also apply to voice-controlled interfaces (e.g. used for smart speakers) or gesture-based interfaces (e.g. used in virtual reality). The term “user journey” corresponds to the series of actions or steps for users to perform in order to reach their goal which, on social networks, can be things such as browsing their feed, sharing a post, setting their preferences, etc. The term “user experience” corresponds to the overall experience users have with social media platforms, which includes the perceived utility, ease of use and efficiency of interacting with it. User interface design and user experience design have been evolving continuously over the last decade. More recently, they have settled for ubiquitous, customised and so-called seamless user interactions and experiences: the perfect interface should be highly personalised, easy to use and multimodal.<sup>4</sup> Even though those trends might increase the ease of use of digital services, they can be used in such a way that they primarily promote user behaviours that run against the spirit of the GDPR.<sup>5</sup> This is especially relevant in the context of the attention economy, where user attention is considered a commodity. In those cases, the legally permissible limits of the GDPR may be exceeded and the interface design and user experience design leading to such cases are described below as “deceptive design patterns”.
  3. In the context of these Guidelines, “deceptive design patterns” are considered interfaces and user journeys implemented on social media platforms that aim to influence users into making unintended, respectively unwilling, and/or potentially harmful decisions, often toward an option that is against the users’ best interests and in favour of the social media platforms interest, with regard to their personal data. Deceptive design patterns aim to influence users’ behaviours, generally relying on cognitive biases, and can hinder their ability “to effectively protect their personal data and make conscious choices”,<sup>6</sup> for example by making them unable “to give an informed and freely given consent”.<sup>7</sup> This can be exploited in several aspects of the design, such as interfaces’ colour choices and placement of the content. Conversely, by providing incentives and user-friendly designs, the realisation of data protection regulations can be supported.
  4. Deceptive design patterns do not necessarily only lead to a violation of data protection regulations. Deceptive design patterns can, for example, also violate consumer protection regulations. The boundaries between infringements enforceable by data protection authorities and those enforceable by national consumer protection, competition or other authorities, can overlap.<sup>8</sup> Under the GDPR,

---

<sup>4</sup> For more details see CNIL, IP Report No. 6: Shaping Choices in the Digital World, 2019. p. 9

[https://www.cnil.fr/sites/default/files/atoms/files/cnil\\_ip\\_report\\_06\\_shaping\\_choices\\_in\\_the\\_digital\\_world.pdf](https://www.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf).

<sup>5</sup> CNIL, Shaping Choices in the Digital World, 2019. p. 10.

<sup>6</sup> CNIL, Shaping Choices in the Digital World, 2019. p. 27.

<sup>7</sup> See Norwegian Consumer Council, *Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy*, p. 10 <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf>, but also CNIL, Shaping Choices in the Digital World, p. 30, 31.

<sup>8</sup> In this regard, Article 25 (2) of the Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), clarifies that the prohibition of deceiving or manipulating designs of online interfaces under its Article 25 (1) shall not apply to practices covered by Directive 2005/29/EC (Directive concerning unfair business-to-consumer commercial practices directive, UCPD) or the

data protection authorities are responsible for sanctioning the use of deceptive design patterns if they actually violate data protection standards and thus the GDPR. Breaches of GDPR requirements need to be assessed on a case-by-case basis. Only deceptive design patterns that might fall within this regulatory mandate are covered by these Guidelines. For this reason, in addition to examples of deceptive design patterns, the Guidelines also present best practices that can be used to design user interfaces which facilitate the effective implementation of the GDPR. Such best practices can offer a first step towards a standardised way for users to effectively control their data and exercise their rights.

5. The deceptive design patterns<sup>9</sup> addressed within these Guidelines result from an interdisciplinary analysis of existing interfaces and can be divided into the following categories:

**Overloading:** users are confronted with an avalanche/ large quantity of requests, information, options or possibilities in order to prompt them to share more data or unintentionally allow personal data processing against the expectations of data subject.

**Skipping:** designing the interface or user journey in a way that the users forget or do not think about all or some of the data protection aspects.

**Stirring:** affects the choice users would make by appealing to their emotions or using visual nudges.

**Obstructing:** an obstruction or blocking of users in their process of getting informed or managing their data by making the action hard or impossible to achieve.

**Fickle:** the design of the interface is inconsistent and not clear, making it hard for users to navigate the different data protection control tools and to understand the purpose of the processing.

**Left in the dark:** an interface is designed in a way to hide information or data protection control tools or to leave users unsure of how their data is processed and what kind of control they might have over it regarding the exercise of their rights.

6. In addition to regrouping deceptive design patterns in these categories according to their effects on users' behaviour, these patterns can also be divided into content-based and interface-based patterns to more specifically address aspects of the user interface or user journey. Content-based patterns refer to the actual content and therefore also to the wording and context of the sentences and information components. In addition, however, there are also components that have a direct influence on the perception of these factors. These interface-based patterns are related to the ways of displaying the content, navigating through it or interacting with it.
7. It is essential to keep in mind that deceptive design patterns raise additional concerns regarding potential impact on children,<sup>10</sup> registering with the social media platform, and also other vulnerable groups of people such as the elderly, persons who are visually impaired, or not as digitally literate as others. Vulnerable groups such as elderly users are often not only less capable to identify manipulative design practices, but also less aware that their digital behaviour is subject to influence. The GDPR requires additional safeguards when the processing is about children's personal data, as the latter may be less aware of the risks and consequences concerned their rights to the processing.<sup>11</sup>

---

GDPR. Also, EU Commission Notice (2021/C 526/01) offers Guidance on the interpretation and application of the UCPD, including on "dark patterns" in its Section 4.2.7.

<sup>9</sup> Categories of deceptive design patterns and types of deceptive design patterns within these categories will be displayed in ***bold and italics*** in the text of the Guidelines. A detailed overview is provided in the Annex.

<sup>10</sup> See also Recital 81, phrase 4, of Regulation (EU) 2022/2065 (Digital Services Act).

<sup>11</sup> GDPR, Recital 38.

Recital 58 explicitly states that where processing is addressed to a child, any information should be given in a clear and plain language that children can easily understand. In addition, the GDPR explicitly includes the processing of individuals' data, particularly those of children, to be among the situations where the risk to the rights and freedoms of individuals of varying likelihood and severity, may result from data processing that could lead to physical, material or non-material damage.<sup>12</sup>

8. Keeping the above in mind, it should be understood that deceptive design patterns are not unique to social media platforms. Strong opinions on this issue were voiced during the public consultation of these Guidelines. Interfaces are present in many other instances where users interact with products and services based on or related with data processing operations. These may include websites and cookie banners,<sup>13</sup> online shops, video games, mobile applications and micropayments etc. Although the deceptive design patterns described below may not be present in the exact same form, their variations may still infringe upon the rights of data subjects or consumers. Nevertheless, these Guidelines focus solely on deceptive design patterns in social media platforms, as influence of these platforms on daily life of people and nations is constantly growing, which has been made clear in previous EDPB documents.<sup>14</sup>

## 2 PRINCIPLES APPLICABLE – WHAT TO KEEP IN MIND?

9. Regarding the data protection compliance of user interfaces of online applications within the social media sector, the data protection principles applicable are set out within Article 5 GDPR. The principle of fair processing laid down in Article 5 (1) (a) GDPR is a starting point for an assessment of existence of deceptive design patterns. As the EDPB already stated, fairness is an overarching principle which requires that personal data shall not be processed in a way that is detrimental, discriminatory, unexpected or misleading to the data subject.<sup>15</sup> If the interface has insufficient or misleading information for users and fulfils the characteristics of deceptive design patterns, it can be classified as unfair processing. The fairness principle has an umbrella function and all deceptive design patterns would not comply with it irrespectively of compliance with other data protection principles.
10. Besides this fundamental provision of fairness of processing, the principles of accountability, transparency and the obligation of data protection by design stated in Article 25 GDPR are also relevant regarding design framework and deceptive design patterns could infringe those provisions. However, it is also possible that the legal assessment of deceptive design patterns can be based on the elements

---

<sup>12</sup> GDPR, Recital 75; see also EDPB Guidelines 8/2020 on targeting of social media users, para. 16 [https://edpb.europa.eu/system/files/2021-04/edpb\\_guidelines\\_082020\\_on\\_the\\_targeting\\_of\\_social\\_media\\_users\\_en.pdf](https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf).

<sup>13</sup> Caused by a series of complaints received from NOYB, an EDPB Taskforce has exchanged views on a number of design elements in cookie banners. The common denominator agreed by the SAs in their interpretation of the applicable multi-layered legal framework has been summarized in a "Report of the work undertaken by the Cookie Banner Taskforce" of 17 January 2023, available at [https://edpb.europa.eu/system/files/2023-01/edpb\\_20230118\\_report\\_cookie\\_banner\\_taskforce\\_en.pdf](https://edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf).

<sup>14</sup> EDPB Guidelines 8/2020 on the targeting of social media users, Statement 2/2019 on the use of personal data in the course of political campaigns [https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-22019-use-personal-data-course-political\\_en](https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-22019-use-personal-data-course-political_en).

<sup>15</sup> EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, version 2.0, adopted on 20 October 2020, p. 16; [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).

on general definitions such as Article 4 (11) GDPR, the definition of consent or other specific obligations such as Article 12 GDPR. Article 12 (1) phrase 1 GDPR requires controllers to take appropriate measures to provide any communication related to data subject rights, as well as any information, in a concise, transparent, intelligible and easily accessible form, using clear and plain language. As Recital 39 phrase 3 on the principle of transparency shows, this requirement is not, however, limited to data protection notices<sup>16</sup> or data subject rights,<sup>17</sup> but rather applies to any information and communication relating to the processing of personal data. Phrase 5 of the Recital also clarifies that data subjects 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.

11. For the design of user interfaces of online applications, it is also important to take into account the principle of purpose limitation under Article 5 (1) (b) GDPR, as well as the principle of data minimisation under Article 5 (1) (c) GDPR. In any case, to ensure data protection compliance, controllers are well-advised to double-check compliance with all data protection principles under the GDPR.

## 2.1 Accountability

12. The accountability principle has to be reflected in every user interface design.
13. Article 5 (2) GDPR states that a controller shall be responsible for, and be able to demonstrate compliance with the GDPR principles which are described in Article 5 (1) GDPR. Therefore this principle is closely linked to the relevant principles mentioned above. Accountability can be provided by elements that provide proof of the social media provider's compliance with the GDPR. The user interface and user journey can be used as a documentation tool to demonstrate that users, during their actions on the social media platform, have read and taken into account data protection information, have freely given their consent, have easily exercised their rights, etc. Qualitative and quantitative user research methods, such as A/B testing, eye tracking or user interviews, their results and their analysis can also be used to support demonstration of compliance. It is important to note that such research methods often also involve processing of personal data, which therefore needs to be in line with the GDPR. If, for example, users have to tick a box or click on one of several data protection options, screenshots of the interfaces can serve to show the users' pathway through the data protection information and explain how users are making an informed decision. Results of user research made on this interface would bring additional elements detailing why the interface is optimal in reaching an information goal.

14. In the area of user interfaces, such documentary elements can be found in the disclosure of certain agreements and, above all, when evidence, for example of giving consent or a confirmation of reading, is obtained.

## 2.2 Transparency

15. The transparency principle in Article 5 (1) (a) GDPR has a large overlap with the area of general accountability. Even though controllers have to protect certain sensitive business information towards third parties, making documentation on processing accessible or recordable could help provide accountability: Confirmation of reading can be obtained, for example, for a text which the controller must make available in accordance with the principle of transparency. This can always serve at the same time to ensure transparency towards data subjects.

---

<sup>16</sup> Addressed in part 3.2. – use case 2a of these Guidelines.

<sup>17</sup> Addressed in use cases 4 and 5, i.e. parts 3.4 and 3.5 of these Guidelines.

16. All the data protection principles set out in Article 5 GDPR are specified further in the GDPR. Article 5 (1) (a) GDPR stipulates that personal data shall be processed in a transparent manner in relation to the data subject. The Guidelines on Transparency specify the elements of transparency as laid down by Article 12 GDPR, i. e. the need to provide the information in a “concise, transparent, intelligible and easily accessible form, using clear and plain language”.<sup>18</sup> These Guidelines also provide guidance on how to fulfil the information obligations under Articles 13 and 14 GDPR regarding social media providers.
17. In addition, the text of the data protection principles of Article 5 (1) (a) GDPR and other special legal provisions within the Regulation contain many more details of the principle of transparency, which are linked to specific legal principles, such as the special transparency requirements in Article 7 GDPR for obtaining consent.

### 2.3 Data protection by design and default

18. Article 25 (1) GDPR specifies that controllers shall implement appropriate technical and organisational measures, which are designed to implement data-protection principles, whereas Article 25 (2) GDPR clarifies that such measures shall also be implemented for ensuring that, by default, only personal data which are necessary for each specific processing purpose are processed. In the context of the Guidelines 04/2019 on Article 25 Data Protection by Design and by Default, there are some key elements that controllers and processors have to take into account when implementing data protection by design regarding a social media platform. One of them is that with regard to the principle of fairness, the data processing information and options should be provided in an objective and neutral way, avoiding any deceptive or manipulative language or design.<sup>19</sup> The Guidelines identify elements of the principles for Data Protection by Default and Data Protection by Design, among other things, which become even more relevant with regard to deceptive design patterns:<sup>20</sup>
  - Autonomy – Data subjects should be granted the highest degree of autonomy possible to determine the use made of their personal data, as well as autonomy 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.
  - Consumer choice – The controllers 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 GDPR.
  - 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 deception – Data processing information and options should be provided in an objective and neutral way, avoiding any deceptive or manipulative language or design.

---

<sup>18</sup> Article 29 Working Party Guidelines on transparency under Regulation 2016/679, endorsed by the EDPB [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>19</sup> See Guidelines 04/2019 on Article 25 Data Protection by Design and by Default, p. 18, para. 70.

<sup>20</sup> Excerpt - for the full list, see Guidelines on Article 25 Data Protection by Design and by Default, para. 70.

- Truthful – the controllers must make available information about how they process personal data, should act as they declare they will and not mislead data subjects.
19. Compliance with Data Protection by Default and Data Protection by Design is important when assessing deceptive design patterns, as it would result in avoiding them in the first place. Indeed, confronting one's service and associated interfaces to the elements comprising Data Protection by Default and by Design principles, such as the ones mentioned above, will help identify aspects of the service that would constitute a deceptive design pattern before launching the service. For example, if data protection information is provided without following the principle "No deception", then it is likely to constitute a ***Hidden in Plain Sight*** or ***Emotional Steering*** deceptive design pattern that will both be further developed in use case 1.

### 3 THE LIFE CYCLE OF A SOCIAL MEDIA ACCOUNT: PUTTING THE PRINCIPLES INTO PRACTICE

20. The GDPR applies to the entire course of personal data processing by automated means.<sup>21</sup> In the case of processing of personal data as part of the operation of social media platforms, this leads to the application of the GDPR and its principles to the entire life cycle of a user account.

#### 3.1 Opening a social media account

Use case 1: Registering an account

##### a. Description of the context

21. The first step users need to take in order to have access to a social media platform is signing up by creating an account. As part of this registration process, users are asked to provide their personal data, such as first and last name, email address or sometimes phone number. Users need to be informed about the processing of their personal data and they are usually asked to confirm that they have read the privacy notice and agree to the terms of use of the social media platform. This information needs to be provided in a clear and plain language, so that users are in a position to easily understand it and knowingly agree.
22. In this initial stage of the sign-up process, users should understand what exactly they sign up for, in the sense that the object of the agreement between the social media platform and users should be described as clearly and plainly as possible.
23. Therefore, data protection by design must be taken into account by social media providers in an effective manner to protect data subjects' rights and freedoms.<sup>22</sup>

##### b. Relevant legal provisions

24. Social media providers need to make sure that they implement the principles under Article 5 GDPR properly when designing their interfaces. While transparency towards the data subjects is always essential, this is especially the case at the stage of creating an account with a social media platform. Due to their position as controller or processor, social media platforms should provide the information to users when signing up efficiently and succinctly, as well as clearly differentiated from other non-data protection related information.<sup>23</sup> Part of the transparency obligations of the controllers is to inform users about their rights, one of which is to withdraw their consent at any time if consent is the applicable legal basis.<sup>24</sup>
- i. Consent provided at the sign-up process stage
25. As Articles 4 (11) and 7 GDPR, clarified by Recital 32, state, when consent is chosen as the legal ground for the processing, it must be "*freely given, specific, informed and [an] unambiguous indication of the data subject's wishes by which he or she, by statement or by a clear affirmative action, signifies*

---

<sup>21</sup> See Article 2 (1) GDPR.

<sup>22</sup> See Guidelines 04/2019 on Article 25 Data Protection by Design and by Default.

<sup>23</sup> See Guidelines on transparency, para. 8.

<sup>24</sup> Guidelines on transparency, para. 30 and page 39.

*agreement to the processing of personal data relating to him or her".* All these requirements for consent have to be met cumulatively for it to be considered as valid.

26. For social media providers who ask for users' consent for varying purposes of processing, the EDPB Guidelines 05/2020 on consent provide valuable guidance on consent collection.<sup>25</sup> Social media platforms must not circumvent conditions, such as data subjects' ability to freely give consent, through graphic designs or wording that prevents data subjects from exercising said will. In that regard, Article 7 (2) GDPR states that the request for consent shall be presented in a manner which is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language. Users of social media platforms can provide consent for ads or special types of analysis during the sign-up process, and at a later stage via the data protection settings. In any event, as Recital 32 GDPR underlines, consent always needs to be provided by a clear affirmative act, so that pre-ticked boxes or inactivity of the users do not constitute consent.<sup>26</sup>
27. As already highlighted by the EDPB Guidelines on consent, there must be minimum information that users are provided with to meet the threshold of "informed" consent.<sup>27</sup> If this is not the case, the consent acquired during the sign-up process cannot be considered valid under the GDPR, thus rendering the processing unlawful.
28. Users are asked to provide consent to different kinds of purposes (e.g., further processing of personal data). Consent is not specific and therefore not valid when users are not also provided in a clear manner with the information about what they are consenting to.<sup>28</sup> As Article 7 (2) GDPR provides, consent should be requested in a way that clearly distinguishes it from other information, no matter how the information is presented to the data subject. In particular, when consent is requested by electronic means, this consent must not be included in the terms and conditions.<sup>29</sup> Taking into account the fact that a rising number of users access social media platforms using the interface of their smart mobiles to sign up to the platform, social media providers have to pay special attention to the way the consent is requested, to make sure that this consent is distinguishable. Users must not be confronted with excessive information that leads them to skip reading such information. Otherwise, when users are "required" to confirm that they have read the entire privacy policy and agree to the terms and conditions of the social media provider, including all processing operations, in order to create an account, this can qualify as forced consent to special conditions named there. If refusing consent leads to a denial of the service, it cannot be considered as freely given, granularly and specific, as the GDPR requires. Consent that is "bundled" with the acceptance of the terms and conditions of a social media provider does not qualify as "freely given".<sup>30</sup> This is also the case where the controller "ties" the provision of a contract or a service to the consent request, so that it processes personal data that are not necessary for the performance of the contract by the controller.
29. While consent must be expressed by a positive action on the part of the users, lack of consent should be considered the default state, until consent has been given. The expression of the users' refusal

---

<sup>25</sup> EDPB Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1., adopted on 4 May 2020 [https://edpb.europa.eu/sites/default/files/files/file1/edpb\\_guidelines\\_202005\\_consent\\_en.pdf](https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf).

<sup>26</sup> See Court of Justice of the European Union, Judgment from 1 October 2019, *Verbraucherzentrale Bundesverband e.V. v. Planet 49 GmbH*, case C-673/17, para. 62-63.

<sup>27</sup> Guidelines 05/2020 on consent, para. 64; see also below use case 3a in part 3.3. of these Guidelines.

<sup>28</sup> See Guidelines 05/2020 on consent, para. 68.

<sup>29</sup> Guidelines on transparency, para. 8.

<sup>30</sup> See Guidelines 8/2020 on targeting of social media users, para. 57.

should therefore not require any action on their part or should be possible through an action presenting the same degree of simplicity as the one allowing to express their consent.<sup>31</sup>

## ii. Withdrawal of consent - Article 7 (3) of the GDPR

30. In accordance with Article 7 (3) phrase 1 GDPR, users of social media platforms shall be able to withdraw their consent at any time. Prior to providing consent, users shall also be made aware of the right to withdraw the consent, as required by Article 7 (3) phrase 3 GDPR. In particular, controllers shall demonstrate that users have the possibility to refuse providing consent or to withdraw the consent without any detriment. Users of social media platforms who consent to the processing of their personal data with one click, for example by ticking a box, shall be able to withdraw their consent in an equally easy way.<sup>32</sup> This underlines that consent should be a reversible decision, so that there remains a degree of control for the data subject related to the respective processing.<sup>33</sup> The easy withdrawal of consent constitutes a prerequisite of valid consent under Article 7 (3) phrase 4 GDPR and should be possible without lowering service levels.<sup>34</sup> As an example, consent cannot be considered valid under the GDPR when consent is obtained through only one mouse-click, swipe or keystroke, but the withdrawal takes more steps,<sup>35</sup> is more difficult to achieve or takes more time.

## c. Deceptive design patterns

31. Several GDPR provisions pertain to the sign-up process. Therefore, there are a number of deceptive design patterns which can occur when social media providers do not implement the GDPR as appropriate.

### i. Content-based patterns

#### *Overloading - Continuous prompting (Annex I checklist 4.1.1)*

32. The **Continuous prompting** deceptive design pattern occurs when users are pushed to provide more personal data than necessary for the purposes of processing or to agree with another use of their data, by being repeatedly asked to provide additional data or to consent to a purpose of processing. Such repetitive prompts can happen through one or several devices. Users are likely to end up giving in, as they are wearied from having to refuse the request each time they use the platform.

#### **Example 1:**

**Variation A:** In the first step of the sign-up process, users are required to choose between different options for their registration. They can either provide an email address or a phone number. When users choose the email address, the social media provider still tries to convince users to provide the phone number, by declaring that it will be used for account security, without providing alternatives on the data that could be or was already provided by the users. Concretely, several windows pop up throughout the sign-up process with a

<sup>31</sup> See Recital 42, phrase 5, of the GDPR.

<sup>32</sup> See Guidelines on transparency, para. 113 et seq.

<sup>33</sup> Guidelines 05/2020 on consent, para. 10.

<sup>34</sup> Guidelines 05/2020 on consent, para. 114.

<sup>35</sup> See Guidelines 05/2020 on consent, para. 114.

field for the phone number, along with the explanation “*We'll use your [phone] number for account security*”. Although users can close the window, they get overloaded and give up by providing their phone number.

**Variation B:** Another social media provider repeatedly asks users to provide the phone number every time they log into their account, despite the fact that users previously refused to provide it, whether this was during the sign-up process or at the last log-in.

33. The example above illustrates the situation where users are continuously asked to provide specific personal data, such as their phone number. While in variation A of the example, this ***Continuous prompting*** is done several times during the sign-up process, variation B shows that users can also be faced with this deceptive design pattern when they have already registered. To avoid this deceptive design pattern, it is important to be particularly mindful of the principles of data minimisation under Article 5 (1) (c) GDPR and, in cases like the one described in example 1 variation A, also of the principle of purpose limitation under Article 5 (1) (b) GDPR. Therefore, when social media providers state that they will use the phone number “for account security”, they shall only process the phone number for said security purposes and must not further process the phone number in a manner that goes beyond this initial purpose.
34. To observe the principle of data minimisation, social media providers are required not to ask for additional data such as the phone number, when the data users already provided during the sign-up process are sufficient. For example, to ensure account security, enhanced authentication is possible without the phone number by simply sending a code to users' email accounts or by several other means.
35. Social network providers should therefore rely on means for security that are easier for users to re-initiate. For example, the social media provider can send users an authentication number via an additional communication channel, such as a security app, which users previously installed on their mobile phone, but without requiring the users' mobile phone number. User authentication via email addresses is also less intrusive than via phone number because users could simply create a new email address specifically for the sign-up process and utilise that email address mainly in connection with the Social Network. A phone number, however, is not that easily interchangeable, given that it is highly unlikely that users would buy a new SIM card or conclude a new phone contract only for the reason of authentication.
36. One should bear in mind that if the aim of such a request is to prove that users are legitimately in possession of the device used to log into the social network, this goal can be achieved by several means, a phone number being only one of them. Thus, a phone number can only constitute one relevant option on a voluntary basis for users. Finally, users need to decide whether they wish to use this mean as a factor for authentication. In particular, for a one-time-verification, users' phone numbers are not needed because the email address constitutes the regular contact point with users during the registration process.
37. The practice illustrated under example 1 variation A may mislead users and render them to unwillingly provide such information, believing that this is necessary to activate or protect the account. However, in reality users were never provided with the alternative (e.g. use of the email for account activation and security purposes). Under example 1 variation B, users are not informed about a purpose of processing. However, this variation still constitutes a ***Continuous prompting*** deceptive design pattern, as the social media provider disregards the fact that users previously refused to provide the phone

number, and keeps asking for it. When users gain the impression that they can only avoid this repeated request by putting in their data, they are likely to give in.

38. In the following example, users are repeatedly encouraged to give the social media platform access to their contacts:

**Example 2:** A social media platform uses an information or a question mark icon to incite users to take the “optional” action currently asked for. However, rather than just provide information to users who expect help from these buttons, the platform prompts users to accept importing their contacts from their email account by repeatedly showing a pop-up saying “*Let’s do it*”.

39. Particularly at the stage of the sign-up process, this ***Continuous Prompting*** can influence users to just accept the platform’s request in order to finally complete their registration. The effect of this deceptive design pattern is heightened when combined with motivational language as in this example, adding a sense of urgency.
40. The influencing effects of wording and visuals will be further addressed below, when examining the deceptive design pattern ***Emotional Steering***.<sup>36</sup>

#### Obstructing – Misleading action (Annex I checklist 4.4.3)

41. Another example of a situation where social media providers ask for users’ phone numbers without need concerns the use of the platform’s application:

**Example 3:** When registering to a social media platform via desktop browser, users are invited to also use the platform’s mobile application. During what looks like another step in the sign-up process, users are invited to discover the app. When they click on the icon, expecting to be referred to an application store, they are asked instead to provide their number to receive a text message with the link to the app.

42. Explaining to users that they need to provide the phone number to receive a link to download the application constitutes ***Misleading action*** for a number of reasons: First of all, there are several ways for users to use an application, e. g., by scanning a QR code, using a link or by downloading the app from the store for applications. Second, these alternatives show that there is no mandatory reason for the social platform provider to ask for the users’ phone number. When users have completed the sign-up process, they need to be able to use their log-in data (i.e. usually email address and password) to log in regardless of the device they are using, whether they use a desktop or mobile browser or an application. This is underlined even more by the fact that instead of a smartphone, users could wish to install the application on their tablet, which is not linked to a phone number.

#### Stirring – Emotional steering (Annex I checklist 4.3.1)

43. With the ***Emotional Steering*** deceptive design pattern, wordings or visual elements (such as style, colours, pictures or others) are used in a way that conveys information to users in either a highly positive outlook, making users feel good, safe or rewarded, or a highly negative one, making users feel anxious, guilty or punished. The manner in which the information is presented to users influences their

---

<sup>36</sup> See para. 43 et seq. in use case 1, as well as the overview of examples in the Annex checklist.

emotional state in a way that is likely to lead them to act against their data protection interests. Impacts of such practices can be even more effective if based on data collected by the platform. Influencing decisions by providing biased information to individuals can generally be considered as an unfair practice contrary to the principle of fairness of processing set in Article 5 (1) (a) GDPR. It can occur throughout the entire user journey within a social media platform. However, at the sign-up process stage, the steering effect can be especially strong, considering the overload of information that users might have to deal with in addition to the steps needed to complete the registration.

44. In the light of the above, ***Emotional Steering*** at the stage of the registration with a social media platform may have an even higher impact on children, the elderly and other groups (i.e. provide more personal data due to lack of understanding of processing activities), considering their vulnerable nature as data subjects.<sup>37</sup> When social media platform services are addressed to children or other vulnerable data subjects, they should ensure that the language used, including its tone and style, is appropriate so that the vulnerable users, as recipients of the message, easily understand the information provided.<sup>38</sup> Considering the vulnerability of children, the elderly and other data subjects, deceptive design patterns may influence these users to share more information, as “imperative” expressions can make them feel obliged to do so, for example to appear popular among peers or because they believe providing the data is mandatory.
45. When users of social media platforms are prompted to give away their data swiftly, they do not have time to “process” and thus really comprehend the information they are provided with, in order to take a conscious decision. Motivational language used by social media platforms could encourage users to subsequently provide more data than required, when they feel that what is proposed by the social media platform is what most users will do and thus the “correct way” to proceed.

**Example 4:** The social media platform asks users to share their geolocation by stating: “Hey, a lone wolf, are you? But sharing and connecting with others help make the world a better place! Share your geolocation! Let the places and people around you inspire you!”

46. During the sign-up process, the users’ goal is to complete the registration in order to be able to use the social media platform. Deceptive design patterns such as ***Emotional Steering*** have stronger effects in this context. These risk to be stronger in the middle or towards the end of the sign-up process compared to the beginning, as users will most of times complete all the necessary steps “in a rush”, or be more susceptible to a sense of urgency. In this context, users are more likely to accept to put in all the data they are requested to provide, without taking the time to question whether they should do so. In this sense, the motivational language used by the social media provider can have an influence on users’ instant decision, as can the combination of motivational language with other forms of emphasis, such as exclamation marks, as shown in the example below.

**Example 5:** Social media provider incentivises users to encourage them to share more personal data than actually required by prompting users to provide a self-description: “*Tell us about your amazing self! We can’t wait, so come on right now and let us know!*”

47. With this practice, social media platforms receive a more detailed profile of their users. However, depending on the case, providing more personal data, e.g. regarding users’ personality, might not be necessary for the use of the service itself and therefore violate the data minimisation principle as per Article 5 (1) (c) GDPR. As illustrated in example 5, such techniques do not cultivate users’ free will to

---

<sup>37</sup> See also above, para. 7.

<sup>38</sup> See Guidelines on transparency, para. 18.

provide their data, since the prescriptive language used can make users feel obliged to provide a self-description because they have already put time into the registration and wish to complete it. When users are in the process of registering to an account, they are less likely to take time to consider the description they give or even if they would like to give one at all. This is particularly the case when the language used delivers a sense of urgency or sounds like an imperative. If users feel this obligation, even when in reality providing the data is not mandatory, this can have an impact on their “free will”. It also means that the information provided by the social media platform was unclear.

**Example 6:** The part of the sign-up process where users are asked to upload their picture contains a “?” button. Clicking on it reveals the following message: “*No need to go to the hairdresser’s first. Just pick a photo that says ‘this is me’.*”

48. Even if the sentences in example 6 aim to motivate users and to seemingly simplify the process for their sake (i. e. no need for a formal picture to sign up), such practices can impact the final decision made by users who initially decided not to share a picture for their account. Question marks are used for questions, and as an icon, users can expect to find helpful information when clicking on it. When this expectation is not met and users are instead prompted once more to take the action they are hesitant about, consent collected without informing users about the processing of their picture would not be valid, failing to meet the requirements of “informed” and “freely given” consent under Article 7 GDPR in conjunction with Article 4 (11) GDPR. The emotion factor therefore has a strong influence on the legitimacy of consent.

#### ***Obstructing – Longer than necessary (Annex I checklist 4.4.2)***

49. When users try to activate a control related to data protection, but the user journey is made in a way that requires users to complete more steps, compared to the number of steps necessary for the activation of data invasive options, this constitutes the deceptive design pattern ***Longer than necessary***. This pattern is likely to discourage users from activating the data protective controls. In the sign-up process, this can translate into the display of a pop-in or pop-up window asking users to confirm their decision when they choose a restrictive option (e.g. choosing to make their profiles private). The example below illustrates another case of a sign-up process being ***Longer than necessary***.

**Example 7:** During the sign-up process, users who click on the “skip” buttons to avoid entering certain kind of data are shown a pop-up window asking “*Are you sure?*” By questioning their decision and therefore making them doubt it, social media provider incites users to review it and disclose these kinds of data, such as their gender, contact list or picture. In contrast, users who choose to directly enter the data do not see any message asking to reconsider their choice.

Here, asking users for confirmation that they do not want to fill in a data field can make them go back on their initial decision and enter the requested data. This is particularly the case for users who are not familiar with the social media platform functions. This ***Longer than necessary*** deceptive design pattern tries to influence users’ decisions by holding them up and questioning their initial choice, in addition to unnecessarily prolonging the sign-up process, which constitutes a breach of the fairness principle under Article 5 (1) (a) GDPR. The example shows that the deceptive design pattern can bring users to disclose (more) personal data than they initially chose. It describes an imbalance of treatment of users who disclose personal data right away and those who do not: Only those who refuse to disclose the data are asked to confirm their choice, whereas users who do disclose the data are not asked to confirm their choice. This constitutes a breach of the fairness

principle under Article 5 (1) (a) GDPR with regard to users who do not wish to disclose these personal data.

## ii. Interface-based patterns

### ***Stirring – Hidden in Plain Sight (Annex I checklist 4.3.2)***

50. Pursuant to the principle of transparency, data subjects have to be provided with information in a clear way to enable them to understand how their personal data are processed and how they can control them. In addition, this information has to be easily noticeable by the data subjects. However, information related to data protection, in particular links, are often displayed in such a way that users will easily overlook it. Such practices of ***Hidden in plain sight*** use a visual style for information or data protection controls that nudge users away from data protection advantageous options to less restrictive and thus more invasive options.
51. Using small font size or a colour which does not contrast sufficiently to offer enough readability (e. g., faint grey text colour on a white background) can have negative impact on users, as the text will be less visible and users will either overlook it or have difficulties reading it. This is especially the case when one or more eye-catching elements are placed next to the mandatory data protection related information. These interface techniques mislead users and render the identification of information related to their data protection more burdensome and time-consuming, as it requires more time and thoroughness to spot the relevant information.

**Example 8:** Immediately after completing the registration, users are only able to access data protection information by calling up the general menu of the social media platform and browse the submenu section that includes a link to “*privacy and data settings*”. Upon a visit to this page, a link to the privacy policy is not visible at first glance. Users have to notice, in a corner of the page, a tiny icon pointing to the privacy policy, which means that users can hardly notice where the information to the data protection related policies are.

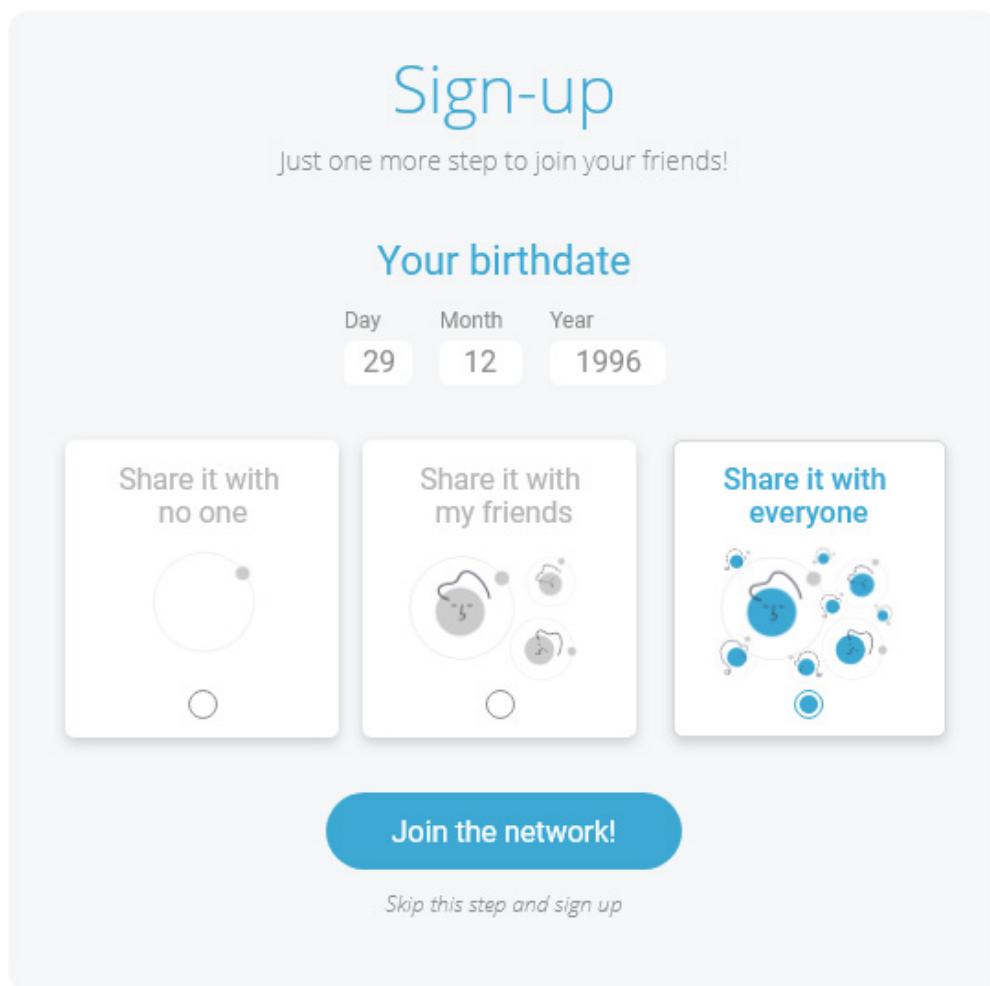
52. It is important to note that even when social media providers make available all the information to be provided to data subjects under Article 13 and 14 GDPR, the way this information is presented can still infringe the overarching requirements of transparency under Article 12 (1) GDPR. When the information is ***Hidden in plain sight*** and therefore likely to be overlooked, this leads to confusion or disorientation and cannot be considered intelligible and easily accessible, contrary to Article 12 (1) GDPR.
53. While the example above shows the deceptive design pattern after completion of the sign-up process, this pattern also already occurs during the sign-up process, as will be shown in the example illustrated below, which combines the ***Hidden in plain sight*** and ***Deceptive snugness*** patterns.

### ***Skipping – Deceptive snugness (Annex I checklist 4.2.1)***

54. Social media providers also need to be mindful of the principle of data protection by default. When data settings are pre-selected, users are subject to a specific data protection level, determined by the provider by default, rather than by users. In addition, users are not always immediately provided with the option to change the settings to stricter, data protection compliant ones. Compliance with the GDPR in this regard does not mean that all options need to look exactly the same. However, if social

media providers highlight one of the options and thus raise the users' attention to it, this needs to be the most restrictive one regarding personal data, in order to comply with, *inter alia*, the principle of data minimisation under Article 5 (1) (c) GDPR.

55. When the most data invasive features and options are enabled by default, this constitutes the pattern ***Deceptive Snugness***. Because of the default effect which nudges individuals to keep a pre-selected option, users are unlikely to change these even if given the possibility. This practice is commonly met in sign-up processes, as illustrated in example 9 below, since it is an effective way to activate data invasive options that users would otherwise likely refuse. Such deceptive design patterns conflict with the principle of data protection by default of Article 25 (2) GDPR, especially when they affect the collection of personal data, the extent of the processing, the period of data storage and data accessibility.<sup>39</sup>



**Example 9:** In this example, when users enter their birthdate, they are invited to choose with whom to share this information. Whereas less invasive options are available, the option "*share it with everyone*" is selected by default, meaning that everyone, i.e. registered users as well as any internet users, will be able to see the users' birthdate.

<sup>39</sup> See also para. 446 of the Final Decision of the Irish Data Protection Authority regarding Instagram (Meta Platforms Ireland Limited) following the EDPB's binding dispute resolution decision of 28 July 2022, [https://edpb.europa.eu/news/news/2022/record-fine-instagram-following-edpb-intervention\\_en](https://edpb.europa.eu/news/news/2022/record-fine-instagram-following-edpb-intervention_en).

56. Example 9 shows a ***Deceptive Snugness*** pattern, as it is not the option offering the highest level of data protection that is selected, and therefore activated, by default. In addition, the default effect of this pattern nudges users to keep the pre-selection, i. e. to neither take time to consider the other options at this stage nor to go back to change the setting at a later stage. The ***Hidden in Plain Sight*** pattern is also used in this interface. Indeed, entering one's birthdate is not mandatory as users can skip this sign-up step by clicking on the link saying "*Skip this step and sign up*" that is available below the "*Join the network!*" button. The fact that the birthdate field and the confirmation button are so prominent is likely to nudge users into entering their birthdate and sending it to the social network because they do not notice the possibility of not sharing this information. This effect would be even stronger if animated circles were used next to the field and button which strongly attract users' attention.
57. Respecting the principle of data protection by design and default does not mean that all options on offer need to look exactly the same. However, if controllers decide to highlight one option more than the other(s), the highlighted one needs to be the most restrictive regarding data processing.
58. Besides nudging users into keeping an option that does not necessarily match their preferences, social media providers might not prompt users to verify or modify their data protection settings according to their preferences after completing the sign-up process. Moreover, changing these default settings could require several steps. When users are not in any way prompted to verify or modify their data protection settings or are not directed in a clear manner to any related information, their data protection level will depend on their own initiative. To facilitate users' control of their data, so-called privacy dashboards can be used that are designed to centralise and ease such endeavour.
59. It is important to keep in mind that the lack of data protection by design and default, in combination with the above-mentioned default effect can have harmful consequences for data subjects, including to their cyber security. Publicly displaying personal data, such as the birthdate, which is used for verification processes by other online services could make it easier for criminals to gain access to users' shopping, banking and other accounts. Another harmful consequence concerns contact possibilities on the social media platform: if the default option for sending contact requests or messages to users is set to "anyone", this raises the risk for cyber-grooming and fraud, especially on vulnerable groups.
60. Finally, when ***Deceptive Snugness*** is applied to the collection of consent, which would equate with considering that users consent by default, for example by using a pre-ticked box or considering inactivity as approval, conditions for consent set in Article 4 (11) GDPR are not met and the processing would be considered unlawful under Articles 5 (1) (a) and 6 (1) (a) GDPR.

#### ***Obstructing – Dead end (Annex I checklist 4.4.1)***

61. It is important to point out that the sign-up process stage is a defining moment for users to get informed. If they are looking for information and cannot find it as no redirection link is available or working, this constitutes a ***Dead end*** pattern because users are left unable to achieve that goal.

**Example 10:** Users are not provided with any links to data protection information once they have started the sign-up process. Users cannot find this information as none is provided anywhere in the sign-up interface, not even in the footer.

62. In practice, this example entails that users will only be able to either stop the registration and go back to the start page if this contains a link to the privacy notice, or to complete the registration, log in to

the social media platform and only then have access to data protection related information. This infringes the principle of transparency and easy access to information that data subjects shall be provided with as required in Article 12 (1) GDPR. It also fails to meet the requirements of Article 13 (1) and (2) GDPR as no information is provided and accessible at the time when personal data are obtained.

63. The **Dead end** pattern can also occur in another way when users are provided with a data protection related action or option during the sign-up process that they cannot find again later, while using the service.

**Example 11:** During the sign-up process, users can consent to the processing of their personal data for advertising purposes and they are informed that they can change their choice whenever they want once registered on the social media by going to the privacy policy. However, once users have completed the registration process and they go to the privacy policy, they find no means or clues on how to withdraw their consent for this processing.

64. In this specific example, users have no mean to withdraw their consent once signed up. Here, the deceptive design pattern **Dead end** infringes the data subjects' right to withdraw consent at any time, and as easily as giving consent, under Article 7 (3) phrases 1 and 4 GDPR.
65. Finally, pointing users to a link that supposedly leads them to data protection related pages, such as settings or data protection information, is also an example of a **Dead end** pattern if the link is broken and no fall-back links are made available that would help users find what they are looking for. This way, users cannot seek for the relevant information, while no explanations are provided to them, such as the reason why this takes place (e.g. technical issues). In such a case, the same issues related to transparency and easy access to information as described in para. 58 occur.

#### d. Best practices

To design user interfaces which facilitate the effective implementation of the GDPR, the EDPB recommends implementing the following best practices for the sign-up process:

**Shortcuts:** Links to information, actions or settings that can be of practical help to users to manage their data and their data protection settings should be available wherever they are confronted to related information or experience (e.g. *links redirecting to the relevant parts of the privacy policy*).

**Contact information:** The company contact address for addressing data protection requests should be clearly stated in the privacy policy. It should be present in a section where users can expect to find it, such as a section on the identity of the data controller, a rights related section or a contact section.

**Reaching the supervisory authority:** Stating the specific identity of the supervisory authority and including a link to its website or the specific website page related to lodging a complaint. This information should be present in a section where users can expect to find it, such as a rights related section.

**Privacy Policy Overview:** At the start / top of the privacy policy, include a (collapsible) table of contents with headings and sub-headings that shows the different passages the privacy notice contains. The names of the single passages clearly lead users regarding the exact content and allow them to quickly identify and jump to the section they are looking for.

**Change spotting and comparison:** When changes are made to the privacy notice, make previous versions accessible with date of release and highlight changes.

**Coherent wordings:** Across the website, the same wording and definition is used for the same data protection. The wording used in the privacy policy should match the one used on the rest of the platform.

**Providing definitions:** When using unfamiliar or technical words or jargon, providing a definition in plain language will help users understand the information provided to them. The definition can be given directly into the text, when users hover over the word, as well as be made available in a glossary.

**Contrasting Data protection elements:** Making data protection related elements or actions visually striking in an interface that is not directly dedicated to the matter. For example, when posting a public message on the platform, controls over association of the geolocation should be directly available and clearly visible.

**Data Protection Onboarding:** Just after the creation of an account, include data protection points within the onboarding experience of the social media provider for users to smoothly discover and set their preferences. For example, this can be done by inviting them to set their data protection preferences after adding their first friend or sharing their first post.

**Use of examples:** In addition to mandatory information clearly and precisely stating the purpose of processing, examples can be used to illustrate a specific data processing to make it more tangible for users.

**Contextual information:** in addition to an exhaustive privacy policy, bring short bits of information at the most appropriate time for the user to have a specific and continuous information on how their data are processed.

### 3.2 Staying informed on social media

Use case 2a: A layered privacy notice

a. **Description of the context**

66. As already highlighted in the Guidelines on transparency, the principle of transparency is very closely linked to the principle of fair processing of personal data.<sup>40</sup> However, information about the processing of personal data also makes data controllers reflect on their own actions, makes data processing more comprehensible for data subjects, and ultimately empowers data subjects to have control over their data, especially by exercising their rights. The resulting equalisation of abilities of the persons involved leads to a fair system of processing personal data. However, more information does not necessarily mean better information. Too much irrelevant or confusing information can obscure important content points or reduce the likelihood of finding them. Hence, the right balance between content and comprehensible presentation is crucial in this area. If this balance is not met, deceptive design patterns can occur.

b. **Relevant legal provisions**

67. The relationships just outlined become clear on the basis of Article 5 GDPR. Transparency and fairness are already systematically mentioned side by side in Article 5 (1) (a) GDPR, as one component determines the other. The fact that not only external but also internal transparency must exist is also made clear by the accountability requirement in Article 5 (2) GDPR. The most important part of internal transparency is the requirement to keep a record of processing activities under Article 30 GDPR. For

---

<sup>40</sup> Guidelines on transparency, p. 4-5.

external transparency, social media providers can provide a layered privacy notice to users, among other means of information.<sup>41</sup> This need for comprehensibility and fair processing also results in the requirements of Article 12 (1) GDPR, which state that any information referred to in Articles 13 and 14 GDPR shall be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Consequently, the information content must be made available without obstacles. If the requirements of Article 12 GDPR are not met, there is no valid information within the meaning of Articles 13 and 14 GDPR. Thus, for effective control, controllers and processors can be held accountable, leading to effectiveness of the GDPR requirements in practice.

c. Deceptive design patterns

i. Content-based patterns

68. Regarding this use case, content-based patterns find their limits in Article 12 (1) GDPR, which requires a precise and intelligible form as well as clear and plain language regarding the information provided.

***Left in the Dark – Conflicting Information (Annex I checklist 4.6.2)***

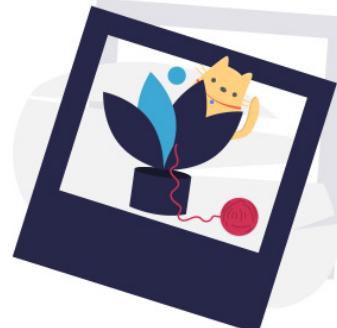
69. One of the most obvious cases where this can occur is when ***Conflicting Information*** is given, which leaves users unsure of what they should do and of the consequences of their actions, therefore not taking any, or keeping the default settings.

### Sharing your information

On our platform you can **share everything and anything!** The more you share, the **more exciting** your **experience** will be! And at any time you can set your preference on the visibility of the information you share on our platform.

For example, you can decide if you want to **share your geolocation** or who will be able to read your posts.

If you **change the publicity of your information** once it is posted online, you will lose visibility and some people might not be able to see it anymore.



**Example 12:** In this example, the information related to data sharing gives a highly positive outlook of the processing by highlighting the benefits of sharing as many data as possible. Coupled to the illustration representing the photograph of a cute animal playing with a ball, this ***Emotional Steering*** can give users the illusion of safety and comfort with regard to the potential risks of sharing some kind of information on the platform. On the other hand, information given on how to control the publicity of one's data is not clear. First it is said that users can set their sharing preference any time they want. Then, however, the last sentence indicates that this is not possible once something has already been posted on the platform. Those pieces of ***Conflicting Information*** leave users unsure of how to control the publicity of their data.

<sup>41</sup> See Use case 2.a in Section 3.2 below.

#### **Fickle – Lacking Hierarchy (Annex I checklist 4.5.1)**

71. Similar effects as with **Conflicting Information** and **Emotional Steering** can occur if the presentation of the information does not follow an internal system or any hierarchy. Information related to data protection which is **Lacking Hierarchy** occurs when said information appears several times and is presented in several different ways. Users are likely to be confused by this redundancy and to be left unable to fully understand how their data are processed and how to exercise control over them. Such architecture makes information hard to understand, as the complete picture is not easily accessible. In cases as the one described in the following example, this infringes the requirements of intelligibility and ease of access under Article 12 (1) GDPR.

**Example 13:** Information related to data subject rights is spread across the privacy notice.

Although different data subject rights are explained in the section “*Your options*”, the right to lodge a complaint and the exact contact address is stated only after several sections and layers referring to different topics. The privacy notice therefore partly leaves out contact details at stages where this would be desirable and advisable.

72. **Lacking Hierarchy** can also emerge when the given information is structured in a way that makes it hard for users to orientate, as the following example shows.

**Example 14:** The privacy policy is not divided into different sections with headlines and content. There are more than 70 pages provided. However, there is no navigation menu on the side or the top to allow users to easily access the section they are looking for. The explanation of the self-created term “*creation data*” is contained in a footnote on page 67.

#### **Left in the Dark – Ambiguous Wording or Information (Annex I checklist 4.6.3)**

73. Even if the choice of words is not overtly contradictory, problems can arise from the use of ambiguous and vague terms when giving information to users. With such information, users are likely to be left unsure of how data will be processed or how to have some control over the data. If it can be assumed that average users would not understand the genuine message of the information without special knowledge, the conditions of Article 12 (1) GDPR are not met. By extension, the use of **Ambiguous wording or information** can contradict the principle of fairness of Article 5 (1) (a) GDPR, since information cannot be considered transparent, making data subjects unable to understand the processing of their personal data and to exercise their rights.

**Example 15:** A privacy notice describes part of a processing in a vague and imprecise way, as in this sentence: “*Your data might be used to improve our services*”. Additionally, the right of access to personal data is applicable to the processing as based on Article 15 (1) GDPR but is mentioned in such a way that it is not clear to users what it allows them to access: “*You can see part of your information in your account and by reviewing what you've posted on the platform*”.

74. In the example, the use of conditional tense (“*might*”) leaves users unsure whether their data will be used for the processing or not. The term “*services*” is likely to be too general to qualify as “*clear*”. In addition, it is unclear how data will be processed for the improvement of services. The EDPB recalls that the use of conditional tense or vague wording does not constitute “*clear and plain language*” as

required by Article 12 (1) phrase 1 GDPR and may only be used if controllers are able to demonstrate that this does not undermine the fairness of processing.<sup>42</sup>

#### **Fickle – Language discontinuity (Annex I checklist 4.5.4)**

75. When online services are offered and addressed to residents of certain Member States, the data protection notices should also be offered in these languages.<sup>43</sup> In this context, it is important that the choice of a particular language can also be switched manually and is implemented continuously without interruptions. If these criteria are not met, data subjects are confronted with a **Language Discontinuity**, leaving them unable to understand information related to data protection. Users will face this deceptive design pattern when data protection information is not provided in the official languages of the country where they live, whereas the service is provided in that language. If users do not master the language in which data protection information is given, they will not be able to read it easily and therefore will not be aware of how their personal data are processed. It is important to note that **Language Discontinuity** can confuse users and create a settings environment that they do not understand how to make use of. This deceptive design pattern can appear in various ways, as will be shown throughout these Guidelines.

##### **Example 16:**

**Variation A:** The social media platform is available in Croatian as the language of users' choice (or in Spanish as the language of the country they are in), whereas all or certain information on data protection is available only in English.

**Variation B:** Each time users call up certain pages, such as the help page, these automatically switch to the language of the country users are in, even if they have previously selected a different language.

76. Variation A illustrates the case where no information is available in a language apparently mastered by the data subject. This means that they cannot read the information and by extension cannot understand how their personal data are processed. Information cannot be considered intelligible as required in Article 12 (1) GDPR. Due to the lack of data protection information in the understandable language, the information required under Article 13 respectively 14 GDPR cannot be considered to have been given to data subjects.
77. Variation B describes a case where data protection information pages are by default presented in the language of the users' country of residence despite their clear language choice. This means that users have to reset their language preference each time they access a data protection information page. This can be considered as an unfair practice towards data subjects and could contribute to a breach of the principle of fairness of Article 5 (1) (a) GDPR.

#### **ii. Interface-based patterns**

78. In some cases, social media providers make use of specific practices to present their data protection settings. During the sign-up process, users are provided with a lot of information and different settings related to data protection. To make sure users can find their way to these settings and make changes

---

<sup>42</sup> See Guidelines on transparency, para. 12, including the "Poor Practice Examples", and para. 13.

<sup>43</sup> See Guidelines on transparency, para. 13 and footnote 15.

at any point when using the platform, the settings should be easily accessible and associated with relevant information for users to make an informed decision. The “easily accessible” element means that data subjects should not have to seek out the information. Regarding privacy policies, the Article 29 Working Party has already stated that a positioning or colour schemes that make a text or link less noticeable, or hard to find on a webpage, are not considered easily accessible.<sup>44</sup>

#### ***Overloading – Privacy Maze (Annex I checklist 4.1.2)***

79. According to the Guidelines on Transparency, the privacy notice should be easily accessible, i.e. through one click on websites.<sup>45</sup> Using the method of layered approach can help present the privacy notice more clearly in the sense of Article 12 (1) GDPR.<sup>46</sup> However, this should not result in making the exercise of important functions or rights unnecessarily difficult by providing a complex privacy policy consisting of innumerable layers that would result in the deceptive design pattern **Privacy Maze**. This pattern corresponds to an information or data protection control being particularly difficult to find, as users have to navigate through many pages without having a comprehensive and exhaustive overview available. This is likely to make users overlook the relevant information/setting or to give up looking for them. The layered arrangement is intended to facilitate readability and give information on how to exercise data subject rights, not to make them more difficult. It is central to ensure that users can easily follow the explanations.
80. In that regard, what is best for users is not a one-size-fit-all approach and depends on many criteria, such as the kind of users on the platform or the general type of design of the application. Where possible, testing the implemented layered approach with users to get their feedback should be carried out to assess its effectiveness. For this reason, no concrete number can be quantified for the maximum number of information layers permissible. It must therefore always be determined on a case-by-case basis whether too many layers are used and thus deceptive design patterns occur. However, the higher the number, the more it can be assumed that users will be discouraged or misled. A high number of layers will only be appropriate for special individual cases in which it is not easy to provide the complex information comprehensively. At the same time, the layered approach may not be misused to hide information in deeper layers or by adding unnecessary layers.
81. However, this is to be assessed differently when it comes to the exercise of the rights of the users. The GDPR requires that the exercise of these rights is always granted. This framework determines the presentation of information on related functions and the exercise of rights. When users want to exercise their rights, the number of steps should be as low as possible. As a result, users should get to the function that allows them to exercise their rights as directly as possible. In most cases, having to navigate a high number of information layers before users can actually exercise their rights through functions could discourage them from exercising these rights. If a high number of steps are implemented, the social media provider should be able to demonstrate the benefit this has for users as data subjects under the GDPR. In addition to the explanation of data subject rights in the privacy notice, as required by Article 13 (2) (b), (c) and (d) GDPR, the exercise of rights should also be accessible independently from this information. For example, users should be able to exercise data subject rights via the platform’s menu as well.

---

<sup>44</sup> Guidelines on transparency, para. 11.

<sup>45</sup> See Guidelines on transparency, example in para. 11.

<sup>46</sup> For details on the layered approach in a digital environment, see Guidelines on transparency, para. 35-37.

**Example 17:** On its platform, the social media provider makes available a document called “*helpful advice*” that also contains important information about the exercise of data subject rights. However, the privacy policy does not contain any link or other hint to this document. Instead, it mentions that more details are available in the Q&A section of the website. Users expecting information about their rights in the privacy policy will therefore not find these explanations there and will have to navigate further and search through the Q&A section.

82. This example clearly shows a ***Privacy Maze*** pattern that makes access to further information to the data subject rights, and in particular on how to exercise them, harder to find than it should, contrary to Article 12 (2) GDPR. In addition, if the privacy policy is incomplete, this also infringes Article 13 (2) (b), (c) and (d), respectively Article 14 (2) (c), (d) and (e) GDPR. Indeed, whereas more detailed information or the direct mean to exercise the rights could be one click away from where they are mentioned in the privacy policy, users in the example will have to navigate to the Q&A and search it in order to find the “*helpful advice*” document.
83. It is important to note that even stronger effects than those caused by too many layers<sup>47</sup> can occur when not only several devices, but also several apps provided by the same social media platform, such as special messenger apps, are used. Users who use that kind of secondary app would face greater obstacles and efforts if they have to call up the browser version or the primary app to obtain data protection related information. In such a situation, which is not only cross-device but cross-application, the relevant information must always be directly accessible no matter how users use the platform.

#### ***Obstructing – Dead end (Annex I checklist 4.4.1)***

84. Violations of legal requirements can also occur when data protection information required by the GDPR is made available through further actions, such as clicking on a link or a button. In particular, misdirected navigation or inconsistent interface design that leads to ineffective features cannot be classified as fair under Article 5 (1) (a) GDPR, as users are misled when they either try to reach some information or set their data protection preferences. ***Dead ends*** where users are left alone without functions to pursue their rights should therefore be avoided in any case and directly violate Article 12 (2) GDPR stating that the controller has to facilitate the exercise of rights.

**Example 18:** In its privacy policy, a social media provider offers many hyperlinks to pages with further information on specific topics. However, there are several parts in the privacy policy containing only general statements that it is possible to access more information, without saying where or how.

85. The privacy policy is generally viewed as the document that centralises all information concerning data protection matters in accordance with the obligations set in Articles 12, 13 and 14 GDPR. Therefore, it is necessary to also ensure redirection to all the relevant places on the social media platform for users to control their data or exercise their rights. In example 18 above, this is only partly implemented, as links to further information are provided for some elements, but not for others. For these, the ***Dead end*** pattern can lead to a breach of Article 12 (1) GDPR, by making some data protection information hard to access, or of Article 12 (2) GDPR, by not facilitating the exercise of the rights.

#### d. Best practices

---

<sup>47</sup> See above, para. 81 and 82.

**Sticky navigation:** While consulting a page related to data protection, the table of contents can be constantly displayed on the screen allowing users to always situate themselves on the page and to quickly navigate in the content thanks to anchor links.

**Back to top:** Include a return to top button at the bottom of the page or as a sticky element at the bottom of the window to facilitate users' navigation on a page.

**Shortcuts:** see use case 1 for definition (p. 22). (e.g. *in the privacy policy, provide for each data protection information links that directly redirects to the related data protection pages on the social media platform*).

**Contact information:** see use case 1 for definition (p. 22).

**Reaching the supervisory authority:** see use case 1 for definition (p. 22).

**Privacy Policy Overview:** see use case 1 for definition (p.22).

**Change spotting and comparison:** see use case 1 for definition (p. 22).

**Coherent wordings:** see use case 1 for definition (p. 22).

**Providing definitions:** see use case 1 for definition (p. 22).

**Use of examples:** see use case 1 for definition (p. 22).

Use case 2b: Providing information about joint controllership to the data subject, Article 26 (2) GDPR

a. Description of the context and relevant legal provisions

86. The second phrase of Article 26 (2) GDPR provides for additional transparency provisions in the specific case of joint controllership.<sup>48</sup> These ensure that the essence of the joint controllership agreement is made available to the data subjects.<sup>49</sup> In its Guidelines 07/2020 on the concepts of controller and processor in the GDPR, the EDPB recommends that the essence cover at least all the elements of the information referred to in Articles 13 and 14 GDPR that should already be accessible to data subjects, and to specify for each element which joint controller is responsible for ensuring compliance with it.<sup>50</sup> The essence of the arrangement must also indicate the contact point, if designated. 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.<sup>51</sup>

b. Deceptive design patterns

**Example 19:** With regard to deceptive design patterns, the challenge for controllers in this constellation is to integrate this information into the online system in such a way that it can be easily perceived and does not lose its clarity and comprehensibility, even though Article 12 (1) phrase 1 GDPR does not refer directly to Article 26 (2) phrase 2 GDPR.

<sup>48</sup> For the definition of joint controllership, see Article 4 (7) in conjunction with Article 26 (1) phrase 1 GDPR, as well as the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, adopted on 7 July 2021, version 2.1, para. 46-49, available at

[https://edpb.europa.eu/system/files/2021-07/eppb\\_guidelines\\_202007\\_controllerprocessor\\_final\\_en.pdf](https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf).

<sup>49</sup> See EDPB Guidelines 07/2020 on controller and processor, para. 179.

<sup>50</sup> See EDPB Guidelines 07/2020 on controller and processor, para. 180, also for next sentence.

<sup>51</sup> EDPB Guidelines 07/2020 on controller and processor, para. 181.

However, due to the data protection principles of fairness, transparency and accountability under Article 5 (1) (a) and (2) GDPR, comparable requirements derive as well to the case of joint controllership. When joint controllers provide information about the essence of the arrangement in a privacy notice, this also needs to be done in a clear and transparent way. Therefore, the processing can no longer be assessed as fair if the information about it is made difficult to grasp because links are not provided or the information is spread across several information areas. The deceptive design pattern ***Privacy Maze***<sup>52</sup> could be even more confusing than, generally, in a privacy notice, as users can expect the information according to Article 26 (2) phrase 2 GDPR to be given in one piece. A Social Media Provider always refers to “*creation data*” within the privacy policy and does not use the term personal data. Only on page 90, the layered privacy notice contains the explanation that “*creation data might include personal data of the users*”. The essence of the joint controller agreement provided to data subjects also uses the term “*creation data*”, without explanation. The other joint controller (B) has a definition of personal data in its own privacy policy. However, in its privacy policy section about joint controllership with the social media provider, B only provides a link to the agreement provided by the social media provider, without other explanation.

87. The explanations under Article 26 (2) phrase 2 GDPR are more difficult to conceive when they are no longer coherent. This incoherence effect is amplified when social media platforms use self-created terminology which users do not usually associate with the processing of personal data, as shown in example 19 above. In the example, both of the joint controllers infringe Article 26 (2) phrase (2) GDPR, as well as Article 5 (1) (a) GDPR because the information provided on joint controllership is unclear and therefore not transparent for data subjects.

#### Use case 2c: Communication of a personal data breach to the data subject

##### a. Description of the context and relevant legal provisions

88. To be able to identify and address a data breach, a controller has to be able to recognize one.<sup>53</sup> According to Article 4 (12) GDPR, “personal data breach” means “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”. When it comes to social media controllers, data breaches can happen in several ways. For example, if an attacker manages to access personal data and users’ chat messages. Alternatively, due to a programming failure, an app could access personal data outside the scope of the permissions granted by users. Another example would be that users share pictures under the setting “share with my best friends”, but their pictures are made available to a wider range of people instead. As a last example, a bug could allow a social media platform based on real-time video to share further streaming of content despite the fact that users had previously pressed a button to stop the recording.
89. If a personal data breach occurs, a controller shall, in any event, notify the competent supervisory authority according to Article 33 GDPR, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. If a data breach is likely to result in a high risk to the rights

---

<sup>52</sup> See above, use case 2a, example 17 in these Guidelines.

<sup>53</sup> See also EDPB Guidelines 01/2021 on Examples regarding Data Breach Notification, adopted on 14 December 2021, Version 2.0, para. 4, available at [https://edpb.europa.eu/system/files/2022-01/edpb\\_guidelines\\_012021\\_pdbnotification\\_adopted\\_en.pdf](https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012021_pdbnotification_adopted_en.pdf).

and freedoms of natural persons, the controller shall, in general, also communicate such a breach to the data subjects according to Article 34 (1) and (2) GDPR. In this case, the controller must inform the data subjects without undue delay. This information must describe in clear and plain language the nature of the personal data breach, as Article 12 GDPR also applies. Moreover, this information must contain at least information and measures such as (see also Article 33 (3) (b) to (d) in conjunction with Article 34 (2) GDPR):

- the name and contact details of the data protection officer (DPO), if applicable, or another contact point where more information can be obtained;
- a description of the likely consequences of the personal data 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.<sup>54</sup>

90. Such data breach communications under Article 34 GDPR can also contain deceptive design patterns. For example, if the respective controller provides all the necessary information to the data subjects to inform them about the scope of the data breach but also provides them with unspecific and irrelevant information and the implications and precautionary measures the controller has taken or suggests to take. This partly irrelevant information can be misleading and users affected by the breach might not fully understand the implications of the breach or underestimate the (potential) effects.

#### b. Deceptive design patterns

91. To outline some negative examples, malpractices of data breach notifications, infringing Article 34 GDPR in conjunction with Article 12 GDPR, could occur as follows:

##### i. Content-based patterns

###### *Left in the Dark – Conflicting Information (Annex I checklist 4.6.2)*

###### **Example 20:**

- The controller only refers to actions of a third party, that the data breach was originated by a third party (e.g. a processor) and that therefore no security breach occurred. The controller also highlights some good practices that have nothing to do with the actual breach.
- The controller declares the severity of the data breach in relation to itself or to a processor, rather than in relation to the data subject.

###### *Left in the dark – Ambiguous wording or information (Annex I checklist 4.6.3)*

92. When it comes to the language of the communication of the breach to the data subject, it is crucial for controllers to keep in mind that most recipients will not be used to specific, maybe technical or legal data protection related language.

---

<sup>54</sup> Article 29 Working Party Guidelines on personal data breach notification, endorsed by the EDPB, p. 20  
<https://ec.europa.eu/newsroom/article29/items/612052/en>.

**Example 21:** Through a data breach on a social media platform, several sets of health data were accidentally accessible to unauthorised users. The social media provider only informs users that “*special categories of personal data*” were accidentally made public.

93. This constitutes **Ambiguous wording**, as average users do not understand the term “*special categories of personal data*” and therefore do not know that their health data has been leaked. This is due to the fact that “special” has a very different meaning in general language than “special” in the narrow GDPR-related language use. Average users do not know that under Article 9 (1) GDPR, “*special categories of personal data*” relate to personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, or genetic data, biometric data for the purpose of uniquely identifying a natural person, or to data concerning health or data concerning a natural person’s sex life or sexual orientation. Thus, the designation “*special categories of personal data*” constitutes a deceptive design pattern in this scenario, as it misleads users because it is not accompanied with further explanations. This is an example of a situation in which a controller tries to inform data subjects about the breach, but fails to fully comply with its obligation to communicate the data breach in accordance with Article 34 GDPR because the seriousness of the incident will be underestimated by the average reader. The short information in the example is also not intelligible, as required by Article 34 in conjunction with Article 12 (1) phrase 1 GDPR.

94. Another example of **Ambiguous wording** is the following:

**Example 22:** The controller only provides vague details when identifying the categories of personal data affected, e. g. the controller refers to documents submitted by users without specifying what categories of personal data these documents include and how sensitive they were.

95. It is important to note that this deceptive design pattern can occur in all parts of the data breach notification. Whereas the two above-mentioned examples refer to unclear wording about the affected data categories, the next example shows that the category of affected data subjects could be equally unclear:

**Example 23:** When reporting the breach, the controller does not sufficiently specify the category of the affected data subjects, e. g., the controller only mentions that concerned data subjects were students, but the controller does not specify whether the data subjects are minors or groups of vulnerable data subjects.

96. Finally, the seriousness of the incident can also be underestimated when **Ambiguous information** is given similarly to the example below:

**Example 24:** A controller declares that personal data was made public through other sources when it notifies the breach to the Supervisory Authority and to the data subject. Therefore, the data subject considers that there was no security breach.

## ii. Interface-based patterns

97. Negative examples of a data breach notification, contrary to Article 34 GDPR in conjunction with Article 12 GDPR, can also constitute interface-based deceptive design patterns, as shown in the following:

### ***Skipping – Look over there (Annex I checklist 4.2.2)***

**Example 25:**

- The controller reports through texts that contain a lot of non-relevant information and omit the relevant details.
- In security breaches that affect access credentials and other types of data, the controller declares that the data is encrypted or hashed, while this is only the case for passwords.

98. In this case, even if the relevant details are in the report, data subjects are likely to be deflected from it by an overload of irrelevant information.

**c. Best practices**

**Notifications:** Notifications can be used to raise awareness of users on aspects, change or risks related to personal data processing (e.g. *when a data breach occurred*). These notifications can be implemented in several ways, such as through inbox messages, pop-in windows, fixed banners at the top of the webpage, etc.

**Explaining consequences:** When users want to activate or deactivate a data protection control, or give or withdraw their consent, inform them in a neutral way on the consequences of such action.

**Shortcuts:** see use case 1 for definition (p.22) (e.g. *provide users with a link to reset their password*).

**Coherent wordings:** see use case 1 for definition (p.22).

**Providing definitions:** see use case 1 for definition (p.22).

**Use of examples:** see use case 1 for definition (p.22).

### 3.3 Staying protected on social media

Use case 3a: Managing one's consent while using a social media platform

**a. Description of the context and relevant legal provisions**

99. Social media platform users need to provide their respective consent during different parts of data processing activities, for example before receiving personalized advertisement. As already outlined in the EDPB Guidelines on Targeting of Social Media Users, consent can only be an appropriate legal basis if a data subject is offered control and genuine choice.<sup>55</sup> In addition, according to Article 4 (11) GDPR, consent must be specific, informed and unambiguous.<sup>56</sup> It is important to underline that the requirements for valid consent under the GDPR do not constitute an additional obligation, but are preconditions for lawful processing of users' personal data. Moreover, when online marketing or online tracking methods are concerned, Directive 2002/58/EC (e-Privacy Directive) is applicable. However, the prerequisites for valid consent under the e-Privacy Directive are identical to the provisions related to consent in GDPR.<sup>57</sup>

---

<sup>55</sup> Guidelines 08/2020 on the targeting of social media users, para 51.

<sup>56</sup> See also para. 25-29 above.

<sup>57</sup> See Article 2(f) of Directive 2002/58/EC as well as 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, para 14, [https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-52019-interplay-between-eprivacy\\_en](https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-52019-interplay-between-eprivacy_en).

100. Given the principle of accountability laid down in Article 5 (2) GDPR, as well as the necessity for the controller to be able to demonstrate that data subjects have consented to the processing of their personal data under Article 7 (1) GDPR, it is crucial that the social media provider can prove having properly collected users' consent. This condition can become a challenge to prove, e.g. if users are supposed to provide consent by accepting cookies. Furthermore, data subjects might not always be aware that they are giving consent while they click quickly on a highlighted button or on pre-set options. Nevertheless, as Article 7 (1) GDPR underlines, the burden of proof that users have freely given consent relies on the controller.

**b. Deceptive design patterns**

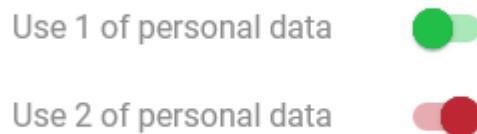
**i. Content-based patterns**

101. In addition to the content-based patterns already explained previously that could apply to the information related to a consent request,<sup>58</sup> two more content-based deceptive design patterns can be found in relation to consent.

***Conflicting Information – Left in the Dark (Annex I checklist 4.6.2)***

**Example 26:** The interface uses a toggle switch to allow users to give or withdraw consent.

However, the way the toggle is designed does not make it clear in which position it is and if users have given consent or not. Indeed, the position of the toggle does not match the colour. If the toggle is on the right side, which is usually associated with the activation of the feature ("switch on"), the colour of the switch is red, which usually signifies that a feature is turned off. Conversely, when the switch is on the left side, usually meaning the feature is turned off, the toggle background colour is green, which is normally associated with an active option.



102. Giving ***Conflicting Information*** when collecting consent makes the information unclear and unintelligible. The example above illustrates a case where the visual information is equivocal. Indeed, confronted to such toggles, users will be unsure if they gave their consent or not. When visual signifiers are mixed up in such a way or presented in other colours that appear contradictory to the actual setting – example 26 containing only one illustration of confusing toggles –, consent cannot be considered as given in an unambiguous way, under Article 7 (2) GDPR, in conjunction with Article 4 (11) GDPR. ***Conflicting Information*** can also be given by textual means as shown below.

<sup>58</sup> See use case 1, para. 32-49, or UC1 example numbers listed in the Annex.

**Example 27:** The social media provider gives contradictory information to users: Although the information first asserts that contacts are not imported without consent, a pop-up information window simultaneously explains how contacts will be imported anyway.

#### ***Obstructing – Misleading action (Annex I checklist 4.4.3)***

103. Besides providing **Conflicting Information**, controllers can implement information that misleads users by not matching their expectations. **Misleading action** is when a discrepancy between information and actions available to users nudges them to do something they do not intend to. The difference between what users expect and what they get is likely to discourage them from going further.

**Example 28:** Users browse their social media feed. While doing so, they are shown advertisements. Intrigued by one ad and curious about the reasons it is shown to them, they click on a “?” sign available on the right bottom corner of the ad. It opens a pop-in window that explains why users see this particular ad and lists the targeting criteria. It also informs users that they can withdraw their consent to targeted advertisement and provides a link to do so. When users click on this link, they are redirected to an entirely different website giving general explanations on what consent is and how to manage it.

104. The case above exemplifies content that does not answer to users’ expectations. Indeed, when users click on the link, they would expect to be redirected to a page that allows them to directly withdraw their consent. The page they are provided with instead does not allow them to do so and does not state the specific way to withdraw their consent on the social media platform. This gap between what users are supposed to find and what they actually find is likely to confuse them and leave them unsure of how to proceed. In the worst case, they could believe they cannot withdraw their consent. Such **Misleading action** cannot be considered transparent as required in Article 12 (1) GDPR. Additionally, comparing withdrawal with the way consent is collected, this practice could infringe Article 7 (3) GDPR if withdrawing consent turns out to be harder than giving it.
105. When social media providers inform users that an action on their part can have a certain consequence and the action actually leads to a different outcome, this constitutes **Misleading action**, as shown in the next example.

**Example 29:** In the part of the social media account where users can share thoughts, pictures, etc., they are asked to confirm that they would like to share this content once they have typed it in or uploaded it. Users can choose between a button saying “*Yes, please.*” and another one saying “*No, thank you.*” However, once users decide against sharing the content with others by clicking on the second button, the content is published on their social media account.

106. As in the previous example, this information is not transparent and takes the users’ choice away from them. Even though users might quickly notice the publication and delete it again, data was processed despite their refusal, and made available to others. A worse example can be found when the processing is not noticeable for users or only with difficulty or knowledge of information technology, because it takes place in the background of the social media platform.

#### **ii. Interface-based patterns**

107. Apart from the two deceptive design patterns above, it is mostly interface-based patterns that are relevant in this use case.

#### ***Skipping – Look over there (Annex I checklist 4.2.2)***

108. When a data protection related action or information is put in competition with another element related or not to data protection, if users choose this other option they are likely to forget about the other, even if it was their primary intent. This is a ***Look over there*** pattern that needs to be assessed on a case-by-case basis.

**Example 30:** A cookie banner on the social media platform states “For delicious cookies, you only need butter, sugar and flour. Check out our favourite recipe here [link]. We use cookies, too. Read more in our cookie policy [link].”, along with an “okay” button.

109. Humour should not be used to misrepresent the potential risks and invalidate the actual information. In this example, users might be tempted to only click on the first link, read the cookie recipe and then click on the “okay” button. Apart from not providing users with a mean not to consent, this example illustrates a case where consent might not be properly informed. Indeed, by clicking on the “okay” button, users might think they just dismiss a funny message about cookies as baked snack and not consider the technical meaning of the term “cookies”. This case would not constitute informed consent in the sense of Article 7 (2) GDPR in conjunction with Article 4 (11) GDPR.
110. Article 7 (2) GDPR further states that a consent request should be clearly distinguishable from other matters. Therefore, it is necessary that the data protection information is not overshadowed by other contexts. In this example, the wordplay based on “cookie” homonyms can make the bakery context outshine the data protection context. For information to be clearly distinguishable, the relevant information for users to provide valid consent should be upfront, not ***Hidden in Plain Sight***, and not mixed with other matters or meanings. No confusion should exist between data protection information and other kinds of content. Otherwise, users might get distracted from the real implications of the processing of their personal data. When implementing these prerequisites, designers need to be given some leeway in order to make the information appealing.

#### ***Obstructing – Dead end (Annex I checklist 4.4.1)***

111. Confusion or distraction is not the only effect possible with deceptive design patterns when it comes to consent. In particular, the ***Dead end*** pattern can interfere in several ways with the conditions for consent set in Article 7 GDPR in conjunction with Article 4 (11) GDPR.

**Example 31:** Users want to manage the permissions given to the social media platform based on consent. They have to find a page in the settings related to those specific actions and wish to disable the sharing of their personal data for research purposes. When users click on the box to untick it, nothing happens at the interface level and they get the impression that the consent cannot be withdrawn.

112. In this specific example, the ***Dead end*** pattern could infringe Article 7 (3) GDPR as users are seemingly left unable to withdraw their consent to the processing of their personal data for research purposes as the mean to do so is apparently not working. If the action of the users is not properly registered within the system, a breach of Article 7 (3) GDPR can be observed. If the choice is actually registered

in the system, the fact that the interface does not reflect the users' action could be considered not respecting the principle of fairness of Article 5 (1) (a) GDPR. When an interface appears to offer the means to properly manage one's consent, by allowing users to give consent or to withdraw a previously given consent, but does not produce any visual effect when interacted with, it is misleading for the user and creates confusion and even frustration for them. Such a gap between the state the system is in and the information conveyed by the interface should be avoided as it can generally hinder users in controlling their personal data.

113. Many processing activities involve several parties, i.e. another (joint) controller or another processor being involved besides the controller or processor the data subject is in direct contact with.

**Example 32:** A social media provider works with third parties for the processing of its users' personal data. In its privacy policy, it provides the list of those third parties without providing a link to each of their privacy policies, merely telling users to visit the third parties websites in order to get information on how these entities process data and to exercise their rights.

114. This example of the **Dead end** pattern shows how access to information about the respective processing is made more difficult for users. Given that they are likely not to receive all the relevant information about the processing it could be considered that such practice infringes the requirements of Article 12 (1) GDPR of easily accessible information. If such practice is used on information provided to collect consent, it can infringe the requirements of informed consent as stated in Article 7 (2) in conjunction with Article 4 (11) GDPR as information would be too difficult to reach, making data subjects not fully aware of the consequences of their choice.

#### ***Obstructing – Longer than necessary (Annex I checklist 4.4.2)***

115. Article 7 (3) GDPR states that the withdrawal of consent should be as easy as giving consent. The Guidelines 05/2020 on consent under Regulation 2016/679 elaborate further on the matter by stating that giving and withdrawing consent should be available through the same mean. This entails using the same interface, but also implies that the mechanisms to withdraw consent should be easily accessible, for example through a link or an icon available at any time while using the social media platform.

**Example 33:** A social media provider does not provide a direct opt-out from a targeted advertisement processing even though the consent (opt-in) only requires one click.

116. The time needed or the number of clicks necessary to withdraw one's consent can be used to assess if it is effectively easy to achieve. Implementing the deceptive design pattern **Longer than Necessary** within the user journey to withdraw their consent, as shown in example 33, goes against these principles, thus breaching Article 7 (3) GDPR.

#### ***Overloading – Privacy Maze (Annex checklist I 4.1.2)***

117. As highlighted in the Guidelines 05/2020 on consent, information on the processing based on consent has to be provided to the data subjects in order for them to make an informed decision.<sup>59</sup> Without it, consent cannot be considered as valid. The same Guidelines further develop the ways to provide

<sup>59</sup> Guidelines 05/2020 on consent, para. 62-64.

information, specifying that layered information can be used to do so. However, as shown in use case 2 a,<sup>60</sup> social media providers need to stay mindful of avoiding the ***Privacy Maze*** deceptive design pattern when providing information related to a consent request in a layered fashion. If some information becomes too difficult to find as data subjects would need to navigate through several pages or documents, consent collected by providing such information could not be considered as informed, going against Article 7 GDPR in conjunction with Article 4 (11) GDPR. By extension, this would mean that the consent is invalid and that the social media provider would breach Article 6 GDPR.

**Example 34:** Information to withdraw consent is available from a link only accessible by checking every section of their account and information associated to advertisements displayed on the social media feed.

118. As the scenario described above shows, the deceptive design pattern ***Privacy Maze*** can also be an issue once consent is collected, by not respecting the condition under Article 7 (3) phrase 4 GDPR, which states that the withdrawal of consent shall be as easy as to give consent. This is specifically due to the fact that the process of withdrawal of consent includes more steps than the affirmative action of providing consent. As the given information is also not easily accessible to the data subject, as it is spread over different parts of the page, the principle as laid down in Article 12 (1) GDPR is violated.

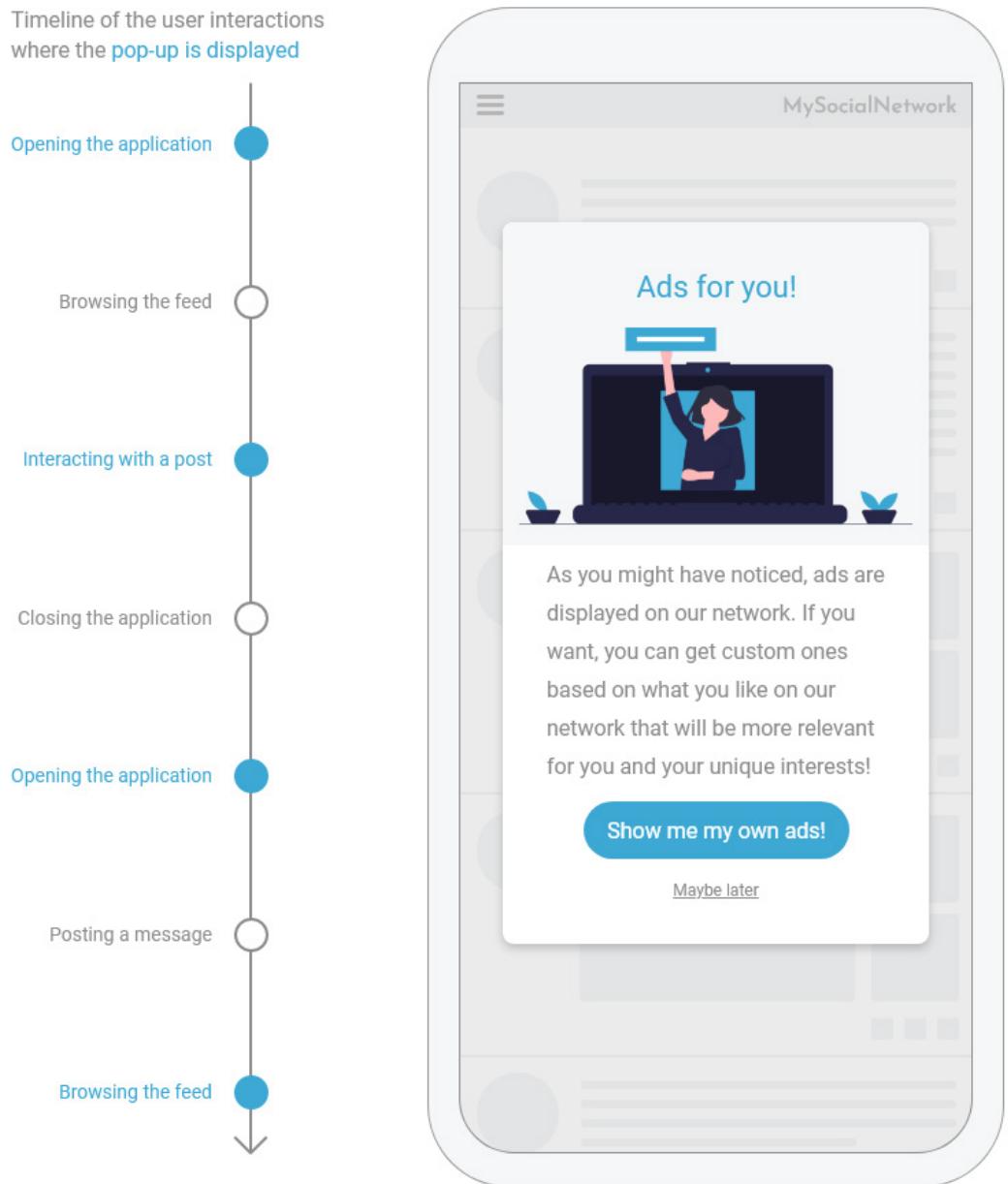
#### ***Overloading – Continuous prompting (Annex I checklist 4.1.1)***

119. ***Continuous Prompting***, when used on users who have not consented to the processing of their personal data for a specific purpose, creates a hindrance in the regular use of the social media. This means that users cannot refuse consent, and by extension withdraw it, without detriment. This contravenes the freely given condition for consent under Article 7 in conjunction with Article 4 (11) GDPR, that consent means any freely given indication of the data subjects' wishes by which they signify agreement to the processing of personal data relating to them. Recital 42 phrase 5 GDPR asserts further that consent cannot be considered freely given if users have no genuine or free choice. This is also supported by the EDPB Guidelines on consent, describing that consent will not be valid if data subjects have no real choice or feel compelled to consent by any element of inappropriate pressure or influence upon them, which prevents them from exercising their free will.<sup>61</sup> As ***Continuous Prompting*** can cause such kind of pressure, this infringes the principle of freely given consent. Additionally, as it is unlikely that once users have consented, the social media provider will regularly (e. g., every time they log back into their account) offer the possibility to withdraw consent, this deceptive design pattern can infringe Article 7 (3) phrase 4 GDPR, laying down that it shall be as easy to withdraw as to give consent ("mirroring effect").

---

<sup>60</sup> See above, para. 79-81.

<sup>61</sup> Guidelines 05/2020 on consent, para. 13-14.



**Example 35:** In this example, when users create their account, they are asked if they accept their data to be processed to get personalised advertising. In case users do not consent at sign-up to this use of their data, they regularly see – while using the social network – the prompting box illustrated above, asking if they want personalised ads. This box is blocking them in their use of the social network. Being displayed on a regular basis, this **Continuous prompting** is likely to fatigue users into consenting to personalised advertisement. Furthermore, in this interface the **Hidden in plain sight** pattern<sup>62</sup> is also used, as the action to accept ads is far more visible than the refusing option.

120. Additionally, the controller could infringe the principle of fairness in the sense of Article 5 (1) (a) GDPR. Given that, in the above example, users did not consent by a clear action to the processing of their personal data for targeted advertisement when creating their account, the repetitive prompting

<sup>62</sup> See above para. 49, or below in part 4.3.2 of the Annex.

constantly putting into question a clear refusal they made is burdensome. This clear action that users took during the registration process is now constantly put into question. The induced degradation of the user experience significantly increases the probability that users will accept the targeted advertisement at some point, just to avoid being asked again every time they log into their account and wish to use the social media platform. In this case, not giving one's consent has a direct impact on the quality of the service given to users and condition the performance of the contract.

### c. Best practices

**Cross-device consistency:** When the social media platform is available through different devices (e.g. computer, smartphones, etc.), settings and information related to data protection should be located in the same spaces across the different versions and should be accessible through the same journey and interface elements (menu, icons, etc.).

**Change spotting and comparison:** see use case 1 for definition (p. 22).

**Coherent wordings:** see use case 1 for definition (p. 22).

**Providing definitions:** see use case 1 for definition (p. 22).

**Use of examples:** see use case 1 for definition (p. 22).

**Sticky navigation:** see use case 2a for definition (p. 28).

**Back to top:** see use case 2a for definition (p. 28).

**Notifications:** see use case 2c for definition (p. 32).

**Explaining consequences:** see use case 2c for definition (p. 32).

## Use case 3b: Managing one's data protection settings

### a. Description of the context

121. After completing the sign-up process, and during the entire life cycle of their social media account, users should be able to adjust their data protection settings.
122. Whether users have prior knowledge of data protection in general and the GDPR in particular or not, and whether they are attentive to the personal data they do or do not wish to share and others to see, they all are entitled to being informed about their possibilities in a transparent manner while using a social media.
123. Users share a lot of personal data on social media platforms. They are often encouraged by the social media platforms to keep sharing more on a regular basis. While users might want to share moments of their life, to participate in a debate on an issue or to broaden their networks of contacts, be it for professional or personal reasons, they also need to be given the tools to control who can see which parts of their personal data. A way to avoid multiplying the number of steps required to change one's setting would be to design a privacy dashboard allowing to centralise the settings and ease the control of users' data.

### b. Relevant legal provisions

124. As mentioned above,<sup>63</sup> as one of the main principles concerning the processing of personal data, Article 5 (1) (a) GDPR stipulates that personal data shall be processed lawfully, fairly and, especially crucial in this regard, in a transparent manner in relation to the data subject (“lawfulness, fairness and transparency”). According to the accountability principle as per Article 5 (2) GDPR, controllers are required to show which measures they are taking to make their processing activities not only lawful and fair, but also transparent. In addition, the principles of minimisation under Article 5 (1) (c) and data protection by design and default under Article 25 GDPR are relevant in this use case.

### c. Deceptive design patterns

#### i. Content-based patterns

125. The first issue that users encounter in this context is where to actually find settings dealing with data protection. Users might read the data protection notice and then decide to make changes related to the processing of their personal data. They could also wish to do so without having read the notice, just through their regular use of the social media, for example when they realise that an information posted on a social media platform (e.g. a photo at the beach with one's family) is shared with an undesired group of people (e.g. co-workers). In any event, the principle of transparency requires the setting options to be easily accessible as well as to be available in an understandable way. This could be achieved by centralising the data and privacy settings in one place using a self-explanatory URL such as [social-network.com]/data-settings.
126. There are several design patterns related to this issue which make it hard for users to find the settings. Social media platform designers therefore ought to be mindful to avoid these deceptive design patterns.

#### ***Overloading – Too many options (Annex I checklist 4.1.3)***

127. Data protection settings need to be easily accessible and ordered logically. Settings related to the same aspect of data protection should preferably be located in a single and prominent location. Otherwise, users will be facing too many pages to check and review which overburdens them in the settings of their data protection preferences. Indeed, confronted with ***Too many options*** to choose from, it can leave them unable to make any choice or make them overlook some settings, finally giving up or missing the settings of their data protection preferences. This infringes the principles of transparency and fairness. In particular, it can infringe Article 12 (1) GDPR as it either makes a specific control related to data protection hard to reach as it is spread across several pages or makes the difference between the different options provided to users unclear.

**Example 36:** Users are likely to not know what to do when a social media platform's menu contains multiple tabs dealing with data protection: “*data protection*”, “*safety*”, “*content*”, “*privacy*”, “*your preferences*”.

128. In this example, the tab titles do not obviously indicate what content users can expect on the associated page or that they all relate to data protection, especially when one of the tab specifically bears this name. This can create the risk of preventing users from making changes. For example, if they would like to restrict or broaden the number of persons who can see the pictures they have uploaded, the tab names could lead them to either click on “*safety*”, if users think there are some safety risks in

<sup>63</sup> See above, para. 1, 9, 10, 14-16.

having their data publicly accessible; “content”, as users wish to set the visibility of their post; or “privacy”, as this specific notion directly relates to what people want to share with others. This means that these titles are not clear enough in regard of the action users would like to achieve. In particular, the terms “data protection” and “privacy” are often used as synonyms and are therefore especially confusing if presented as different sections.

#### ***Left in the dark – Conflicting information (Annex I checklist 4.6.2)***

129. As already described in example 12 and further illustrated in the following example, users can also be given ***Conflicting information*** within the framework of the data protection settings.

**Example 37:** User X switches off the use of their geolocation for advertisement purpose. After clicking on the toggle allowing to do so, a message appears saying “*We've turned off your geolocation, but your location will still be used.*”

#### ***Overloading – Privacy maze (Annex I checklist 4.1.2)***

130. When users change a data protection setting, the principle of fairness also requires social media providers to inform users about other settings that are similar. If such settings are spread across different, unconnected pages of the social media platform, users are likely to miss one or several means to control an aspect of their personal data. Users expect to find related settings next to each other.

**Example 38:** Related topics, such as the settings on data sharing by the social media provider with third parties and vice versa, are not made available in the same or close spaces, but rather in different tabs of the settings menu.

131. There is no “one size fits all approach” when it comes to the average number of steps still bearable for users of social media platforms to take when changing a setting. At the same time, a higher number of steps can discourage users from finalising the change or make them miss parts of it, especially if they want to make several changes. Hindering in such a way the will of users infringes the principles of fairness in Article 5 (1) (a) GDPR. In addition, changing the settings is closely related to the exercise of data subject rights.<sup>64</sup> Changing a data related setting, such as correcting one’s name or deleting one’s graduation year, can be considered an exercise of the right to rectification, respectively right to erasure, for these specific data. The number of steps required should therefore be as low as possible. While it might vary, an excessive number of steps hinders users and therefore infringes the fairness principle, as well as Articles 12 (1) and (2) GDPR.

#### **Fickle – Language Discontinuity (Annex I checklist 4.5.4)**

132. With regard to transparent information, social media platform designers also need to be careful to avoid content-based deceptive design patterns listed in use case 2a, such as ***Language discontinuity***. Not making the setting pages (or parts of them) available in the language users chose for the social media platform makes it harder for them to understand what they can change and therefore set their preferences.

---

<sup>64</sup> See below, Use cases 4 and 5, i.e. parts 3.4. and 3.5. of these Guidelines.

#### **Fickle – Inconsistent Interface (Annex I checklist 4.5.3)**

133. In this context, another issue occurs when social media platforms offer data protection friendly choices to users, but do not inform them about it in a clear manner. This can be the case when the social media platform suddenly differs from its usual design pattern. Such an **Inconsistent Interface** occurs when an interface is not consistent across different contexts or with users' expectations. These differences can lead users not to find the desired control or information or to interact with an element of the interface out of habits even though this interaction leads to make a data protection choice the users do not want.

**Example 39:** Throughout the social media platform, nine out of ten data protection setting options are presented in the following order:

- most restrictive option (i.e. sharing the least data with others)
- limited option, but not as restrictive as the first one
- least restrictive option (i.e. sharing the most data with others).

Users of this platform are used to their data protection settings being presented in this order. However, this order is not applied at the last setting where the choice of visibility of users' birthdays is instead shown in the following order:

- *Show my whole birthday: 15 January 1929* (= least restrictive option)
- *Show only day and month: 15 January* (= limited option, but not the most restrictive one)
- *Do not show others my birthday* (= most restrictive option).

134. In the example, the three choices in the last setting are presented in a different order than the previous settings. Users who have previously changed their other settings are likely to be used to the "usual" order of settings one to nine. At the last setting, they are so used to this order that they instinctively choose the first option, assuming that this must be the most restrictive one. Arranging the options of one data protection setting so differently from the others in the same social media platform is an **Inconsistent Interface** as it plays with what users are used to and their expectations. This can lead to confusion or leave users to think they took the choice they wanted when, in reality, this is not the case.

#### **ii. Interface-based patterns**

135. The second issue one encounters in the context of data protection settings is that the settings might infringe on the principle of data protection by default. Article 25 (1) GDPR requires controllers to take appropriate measures designed to implement data protection principles, such as data minimisation (Article 5 (1) (c) GDPR). These provisions are not respected when the settings on sharing of personal data are pre-set to one of the more invasive options rather than the least invasive one.

#### **Skipping – Deceptive Snugness (Annex I checklist 4.2.1)**

**Example 40:** Between the data visibility options "*visible to me*", "*to my closest friends*" "*to all my connections*", and "*public*", the middle option "*to all my connections*" is pre-set. This means that all users connected to them can see their contributions, as well as all

information entered for signing-up to the social media platform, such as their email address or birthdate.

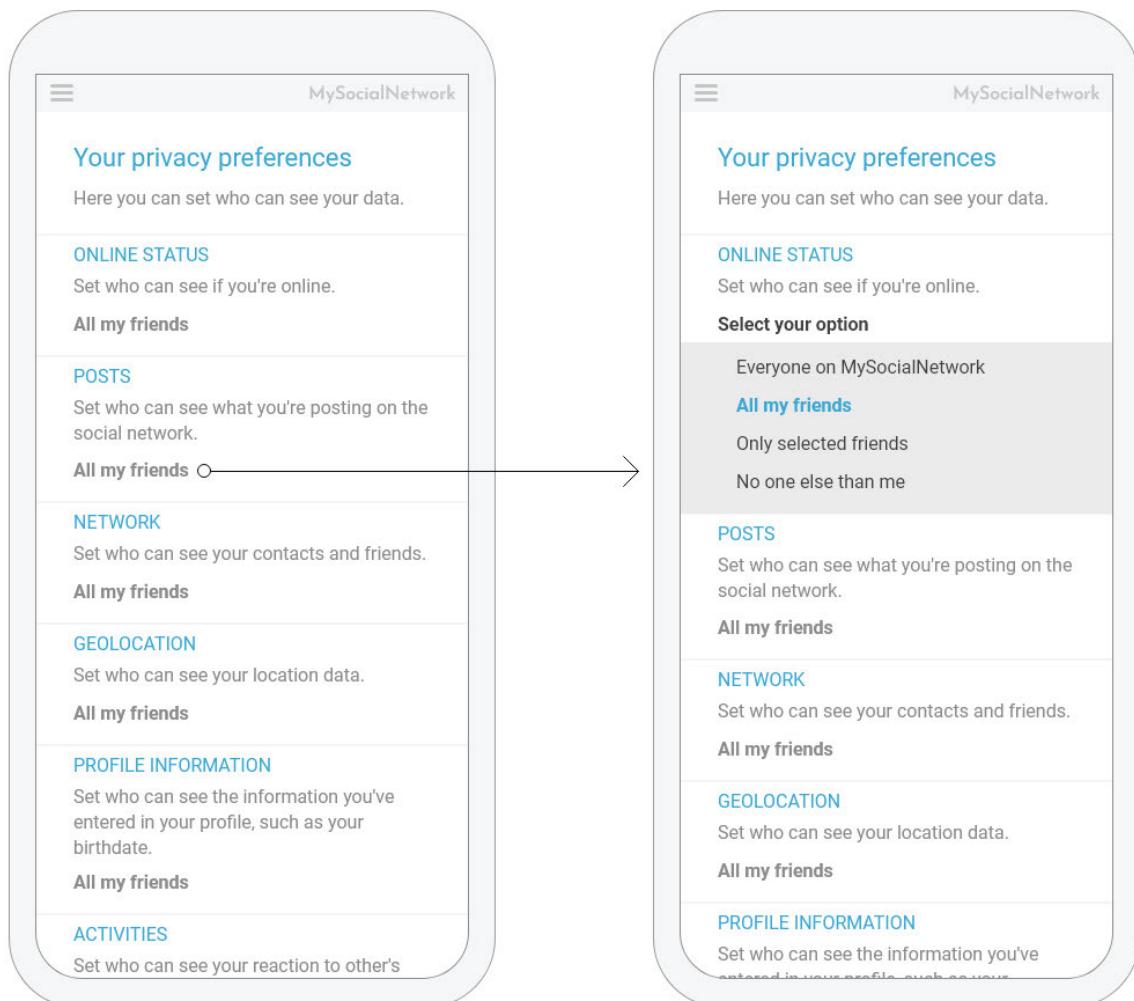
136. Social media providers might argue that the least invasive setting would defeat the goal that users of a particular social media platform have, for example being found by unknown people to find a new buddy, date or job. While this might be true for some particular settings, social media providers need to keep in mind that the fact that users upload certain data on the network does not constitute consent to share this data with others.<sup>65</sup> Where social media providers defer from data protection by default, they will need to be mindful to properly inform users about it. This means that users need to know what the default setting is, that there are less invasive options available and where on the platform they need to go to make changes. In the given example, it means that when the option “*to my closest friends*” is pre-set for contributions users actively post on the social media platform, they should be shown where to change this setting. However, pre-setting the visibility to “*all user connections*” (or even the general public) constitutes **Deceptive Snugness**, especially when it is applied to data the social media provider required from users to create an account, such as the email address or their birthdate. As described in use case 1 para. 55, this practice infringes Article 25 (2) GDPR.

---

<sup>65</sup> For example their birthdate, see para. 58 above.

### **Stirring – Hidden in plain sight (Annex I checklist 4.3.2)**

137. The **Hidden in Plain Sight** and **Deceptive Snugness** deceptive design patterns can easily be combined when it comes to the selection of data protection related options as illustrated in example 9 for the sign-up process, and below when users want to change their data protection preferences while using the social media.



**Example 41:** In this example, when users want to manage the visibility of their data, they have to go in the “*privacy preference*” tab. The information for which they can set their preference is listed there. However, the way that information is displayed does not make it obvious how to change the settings. Indeed, users have to click on the current visibility option in order to access a dropdown menu from which they can select the option they prefer.

138. Even though changing one's preferences is available in this tab, it is **Hidden in plain sight**, as the dropdown menu is not directly visible for users who have to guess that clicking on the current option will open something. There is indeed no usual visual clue (underlined text, down arrow) about the possibility of interacting and opening the dropdown menu. This specific practice is unfair to users and could participate in a general failure to meet the principle of fairness of Article 5 (1) (a) GDPR. Additionally, if the options were pre-selected by default, the deceptive design pattern **Deceptive Snugness** could be also observed, as described above in para. 128.

#### **Fickle – Decontextualising (Annex I checklist 4.5.2)**

139. **Decontextualising** happens when a data protection related information or control is located on a page that is out of context, so that users are unlikely to find it as it would not be intuitive to look for it on that specific page.

**Example 42:** The data protection settings are difficult to find in the user account, as on the first level, there is no menu chapter with a name or heading that would lead in that direction. Users must look up other submenus such as “Security”.

140. In this example, users are not guided to the data protection settings because no meaningful and clear terms are used to indicate where these are on the social media platform. Indeed, the term “Security” only covers a fraction of what can be expected of data protection settings. It is therefore not intuitive for users to look up this menu to find such settings. This lack of transparency makes access to information harder than it should and can be considered as contravening Article 12 (1) GDPR, and potentially Article 12 (2) GDPR if those settings relate to the exercise of a right.

**Example 43:** Changing the setting is hindered since in the social media platform’s desktop version, the “save” button for registering their changes is not visible with all the options, but only at the top of the submenu. Users are likely to overlook it and wrongly assume their settings are saved automatically, therefore moving to another page without clicking on the “save” button. This problem does not occur in the app and mobile versions. Therefore, it creates additional confusion for users moving from the mobile/app to the desktop version, and can make them think they can only change their settings in the mobile version or the app.

141. Once users have found the data protection settings and set their choices, they may not be hindered from doing so. Once users have made a change, the way to save it has to be obvious, whether this happens as soon as users adjust a setting or it needs a confirmation by clicking on a specific element of the interface such as a “save” button. In addition, the principle of fairness under Article 5 (1) (a) GDPR requires social media providers to be consistent throughout their platform, especially across different devices. That is not the case when the interface uses a deceptive design pattern as described in the examples above.

#### **d. Best practices**

**Data protection directory:** For easy orientation through the different section of the menu, provide users with an easily accessible page from where all data protection related actions (e. g., settings) and information are accessible. This page could be found in the social media provider main navigation menu, the user account, through the privacy policy, etc.

**Bulk options:** Putting options that have the same processing purpose together, so that users can change them more easily, while still leaving users the possibility to make more granular changes. If social media platforms present bulk options, these should not contain unexpected or unrelated elements (for example elements with different purposes). If the processing require consent, the bulk options must be in line with the EDPB Guidelines on consent, especially para. 42-44.

**Shortcuts:** see use case 1 for definition (p. 22) (*e.g. when users are informed about an aspect of the processing, they are invited to set their related data preferences on the corresponding setting/dashboard page*).

**Self-explanatory URL:** pages related to data protection settings or information should use a web address that clearly reflects their content. For example, a page centralising data protection control could have a URL such as [social-network.com]/data-settings.

**Coherent wordings:** see use case 1 for definition (p. 22).

**Providing definitions:** see use case 1 for definition (p. 22).

**Use of examples:** see use case 1 for definition (p. 22).

**Sticky navigation:** see use case 2a for definition (p. 28).

**Notifications:** see use case 2c for definition (p. 32).

**Explaining Consequences:** see use case 2c for definition (p. 32).

**Cross-device consistency:** see use case 3a for definition (p. 39).

### 3.4 Staying right on social media: Data subject rights

Use case 4: How to provide proper functions for the exercise of data subject rights

#### a. Description of the context

142. Using a social media platform means taking advantage of its functions along the purposes stated by the social media provider. This also means for users to be able to exercise their data protection rights. They are key elements of data protection and controlling one's own information, regardless of whether data are directly and knowingly provided by data subjects, provided by data subjects by virtue of the use of the service or the device, or inferred from the analysis of data provided by the data subject.<sup>66</sup> The amount of personal data flowing throughout the platform requires enabling users to control their data with the help of the rights provided by the GDPR in a clear and intuitive manner. The EDPB has explained these concepts in several guidelines.<sup>67</sup> The exercise of rights must be available from the beginning until the end of using the platform, and in some cases, even after users have decided to leave the platform and the controller has not yet deleted their data. Non-users of the platform also need to be enabled to exercise data subject rights pertaining to processing of their data. Of course, in some instances not all the data subject rights are available depending on the legal basis for processing the data. The social media provider should therefore also clearly explain why certain rights are not applicable and why some of them may be limited. As mentioned above and in previous chapters the use of rights must be made operative. Automation as well as other functionalities of social media platforms should be used to facilitate the exercise of rights.

#### b. Relevant legal provisions

143. The GDPR describes seven different rights that data subjects can exercise according to certain conditions (e.g. legal basis of the processing, etc.). Article 15 GDPR allows data subjects to know if

---

<sup>66</sup> See Article 29 Working Party Guidelines on the right to data portability under Regulation 2016/679, WP242 rev.01, p. 10, <https://ec.europa.eu/newsroom/article29/items/611233/en>.

<sup>67</sup> Guidelines on the right to data portability and EDPB Guidelines 05/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1) - version adopted after public consultation, [https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-52019-criteria-right-be-forgotten-search-engines\\_en](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-52019-criteria-right-be-forgotten-search-engines_en).

personal data concerning them are processed and to access them, i.e. to obtain further information on their processing, as well as to receive a copy of that data. Article 16 GDPR details the right to rectification allowing data subjects to update the personal data the controller processes. The right to erasure under Article 17 GDPR allows data subjects to obtain the erasure of personal data concerning them. The right to restriction of processing under Article 18 GDPR gives the data subjects the possibility to stop temporarily the processing of their personal data. Article 20 GDPR introduces the right to data portability allowing data subjects to receive their personal data and transmit it to another controller.<sup>68</sup> Data subjects have also the right to object to the processing of their personal data as laid out in Article 21 GDPR. Finally, Article 22 GDPR gives data subjects the right not to be subject of a decision based solely on automated processing.<sup>69</sup>

144. The EDPB underlines that not all of these rights will apply to every social media platform, depending on its legal basis and purposes of processing of personal data and types of services provided. The differences should be explained by the controller in accordance with Article 12 GDPR. This means that the information on applicable rights should be concise and clear to users, including why certain rights do not apply. Such an explanation could limit the amount of communication with users when they are trying to exercise some of them. The exercise of the right should be easy and accessible in accordance with Article 12 (2) and the reply should be given without undue delay as required per Article 12 (3) GDPR. Similarly, the social media platform should explain why certain requests cannot be fulfilled and inform on the possibility to lodge a complaint to a designated supervisory authority as per Article 12 (4) GDPR. Thus, the following deceptive design patterns may not be applicable to all of the rights mentioned above. The right to erasure is discussed in detail in the next chapter.

c. Deceptive design patterns

i. Content-based patterns

Obstructing – Dead end (Annex checklist I 4.4.1)

145. The **Dead end** deceptive design pattern can directly impact the ease of access to the exercise of the rights. When links redirecting to the means to exercise a right are broken or clear explanations on how to exercise a right are missing, users will not be able to properly exercise it, which infringes Article 12 (2) GDPR.

**Example 44:** Users click on “*exercise my right of access*” in the privacy notice, but are redirected to their profile instead, which does not provide any features related to exercising the right.

146. The above-mentioned example of a deceptive design pattern outlines the need to provide users with a clear and intuitive manner to exercise their rights in accordance with Article 12 (1) and (2) GDPR, as they might otherwise not be able to exercise them. It is not enough to confirm to users that they have data subject rights as required per Article 12 (1) GDPR (including the manner of communication) and specifically per Articles 13 (2) (b) and 14 (2) (c) GDPR. Users must also be able to easily exercise them, preferably in a way embedded in the platform’s interface, for example by providing a dedicated form. This would also make the user experience with a platform more positive – seeing that the provider has taken the effort to adapt to users’ expectation of lawful personal data processing and control over

<sup>68</sup> This right is further developed in the Guidelines on the right to data portability.

<sup>69</sup> See also Article 29 Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, wp251rev.01, p. 19 and following,

<https://ec.europa.eu/newsroom/article29/items/612053/en>.

their data by combining the exercise of rights with other functionalities of the service. When the social media platform service allows for a two-way communication among users, as well as between the controller and users, there is no reason for the controller to limit its channel of communication for the facilitation of data subject requests to a separate mean of communication like email. At the same time, data subjects should not be forced to come to the platform to communicate with the controller.<sup>70</sup> In addition, controllers may not limit this data subject right to the right to copy, but instead need to make sure they also provide the information mentioned by Article 15 (1) GDPR to users requesting access to their data.<sup>71</sup>

#### ***Fickle – Language discontinuity (Annex I checklist 4.5.4)***

**Example 45:** When clicking on a link related to the exercise of data subject rights, the following information is not provided in the state's official language(s) of the users' country, whereas the service is. Instead, users are redirected to a page in English.

147. Bearing in mind the principle of transparency under Articles 5 (1) (a) and 12 (1) GDPR, users must receive all the information about their rights in a clear and plain, comprehensible manner. This must also be related to users' location and the language used in that country or jurisdiction in which the service is offered. The fact that users confirm their ability to use a foreign language in any way does not release the controller from its obligations. The same applies when such knowledge of other languages understood by the users can be inferred from their activities. The information should be relevant and helpful to users exercising their rights.

#### ***Left in the dark – Ambiguous wording or information (Annex I checklist 4.6.3)***

148. In the context of data subject rights, users can also be confronted with the deceptive design pattern **Ambiguous wording or information**, as shown in the following example.

**Example 46:** The social media platform does not explicitly state that users in the EU have the right to lodge a complaint with a supervisory authority, but only mentions that in some – without mentioning which – countries, there are data protection authorities which the social media provider cooperates with regarding complaints.

149. Social media providers also need to be mindful to avoid the **Ambiguous wording or information** deceptive design pattern when informing data subjects about their rights. Giving information to users in a way that makes them unsure of how their data will be processed or how to have some control over their data and thus how to exercise their rights infringes the principle of transparency. Additionally, vague wording is not concise language as required by Article 12 (1) GDPR and can make the information provided to the data subject incomplete, which could be considered a breach of Article 13 GDPR. The above-mentioned example also shows an infringement of Article 13 (2) (d) GDPR which requires controllers to provide data subjects with information about their right to lodge a

---

<sup>70</sup> See EDPB Guidelines 01/2022 on data subject rights – right of access, para. 136, version 1.0, [https://edpb.europa.eu/system/files/2022-01/edpb\\_guidelines\\_012022\\_right-of-access\\_0.pdf](https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf).

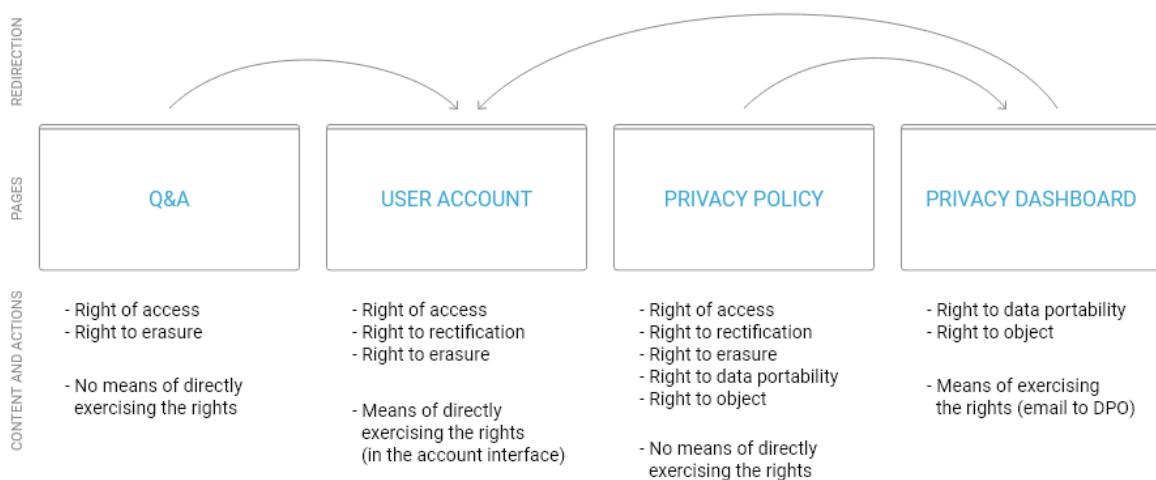
<sup>71</sup> See EDPB Guidelines 01/2022, para. 131, 142, 145.

complaint with a supervisory authority. By extension, this is also contrary to Article 12 (2) GDPR because the social media provider does not facilitate the exercise of the right to lodge a complaint.

## ii. Interface-based patterns

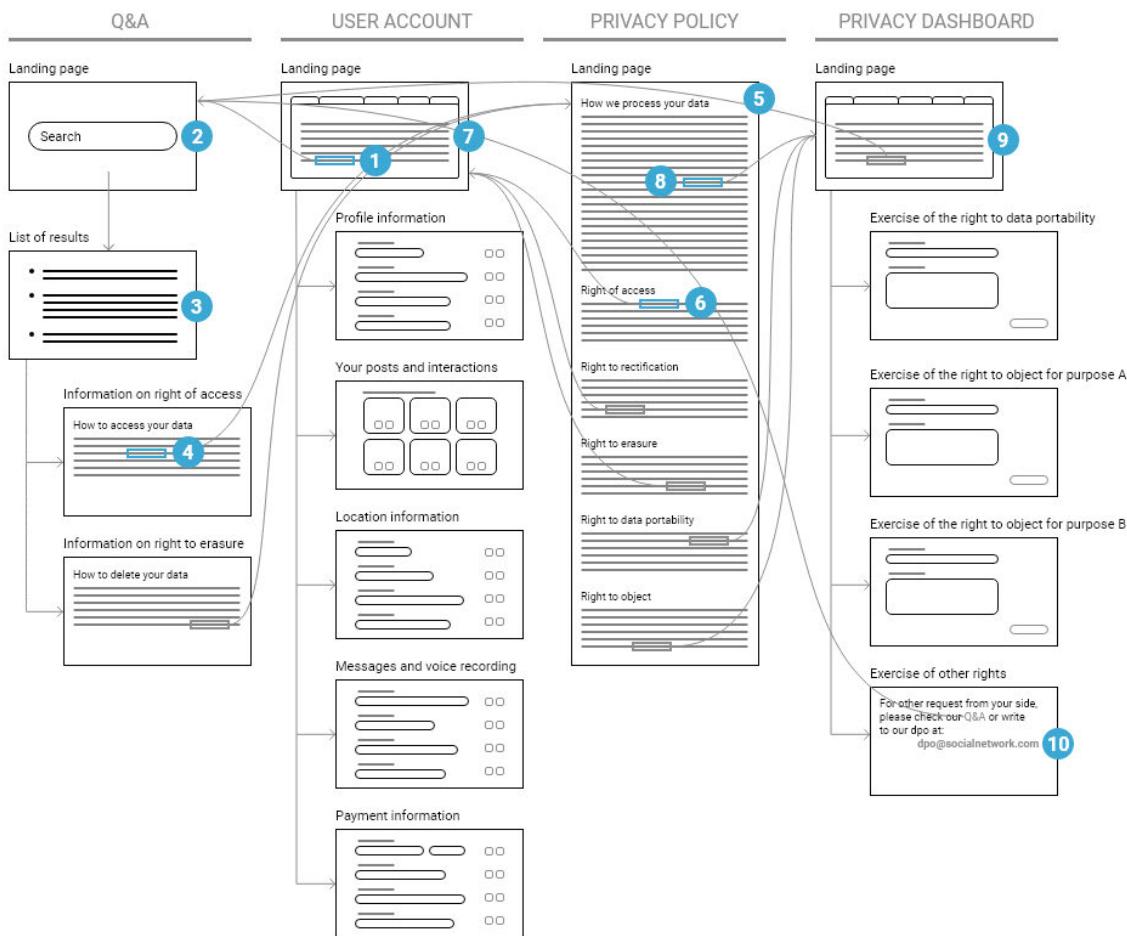
### *Overloading – Privacy Maze (Annex I checklist 4.1.2)*

150. As described earlier in use case 3b, the number of steps necessary to receive the relevant data protection information shall not be excessive, and neither may the number of steps to achieve the data subject rights.<sup>72</sup> Thus, users should always be able to reach the rights exercise site quickly, no matter which starting point they came from and where the social media platform has located this feature. Social media providers should therefore think carefully about the different situations from which users would like to exercise their rights and design access to the place where they can do so accordingly. This means that several paths to reach a data subject right can be created and available on a social media platform. However, each path should facilitate the access to the exercise of the rights and should not interfere with another path. If not, it would be considered to be a **Privacy Maze** deceptive design pattern, as illustrated in examples 47 and 48, contrary to Article 12 (2) GDPR.



**Example 47:** Here, information related to data protection rights is available on at least four pages. Even though the privacy policy informs on all the rights, it does not redirect to the relevant pages for each of them. Conversely, when users visit their account, they will not find any information on some of the rights they can exercise. This **Privacy Maze** forces users to dig through many pages in order to find where to exercise each right and, depending on their browsing, they might not be aware of all the rights they have.

<sup>72</sup> See above, para. 123.



**Example 48:** In this example, users wish to update some of their personal data but do not find a way to do it in their account. They click on a link (1) redirecting them to the Question & Answer page where they enter their question (2). Several results appear (3), some related to the rights of access and deletion. After checking all results, they click (4) on the link available in the “How to access your data” page. It redirects them to the privacy policy (5). There, they find information on additional rights. After reading this information, they click (6) on the link associated with the exercise of the right to rectification which redirects them to the user account (7). Unsatisfied, they go back to the privacy policy and click on a general link “Send us a request” (8). This brings users to their privacy dashboard (9). As none of the available options seem to match their need, users eventually go to the “exercise of other rights” page (10) where they finally find a contact address.

151. Both examples illustrate particularly lengthy and tiresome paths to exercise one's rights. When the means of exercising different rights are not located in the same space but a page listing all the data subject rights is available, the latest should redirect precisely to those different spaces, not only to one or part of them as illustrated in example 47. The other example shows a journey where users do not find the mean to easily exercise the specific right they wish, namely the right to rectification, as the place where it is commonly carried out, namely the user account, does not provide the mean to do so.

Looking for another way to exercise this right, they cannot find a specifically corresponding one and have to turn to a general mean provided in the privacy dashboard.

152. When several paths to the exercise of a right have been designed, it should always be easy for users to find the overview about the data subject rights. Privacy policies should be clear and could serve as one of the gateways to pages where users can exercise their rights. This document should include all of the rights that are applicable. If any of them should be unavailable due to legal or technical limitations this should also be explained, so that users are informed properly. Understanding the limitations of processing operations, either due to their basis or safeguards adopted by controllers, is helpful not only to users. It also limits the instances in which a social media provider has to explain why it cannot comply with a data subject rights request made by users.

#### ***Stirring – Hidden in plain sight (Annex I checklist 4.3.2)***

153. Affecting users' ability to reach the place where to exercise their right can also be done by making related information or links hardly visible using the ***Hidden in Plain Sight*** deceptive design pattern.

**Example 49:** The paragraph under the subtitle “right to access” in the privacy policy explains that users have the right to obtain information under Article 15 (1) GDPR. However, it only mentions users’ possibility to receive a copy of their personal data. There is no direct link visible to exercise the copy component of the right of access under Article 15 (3) GDPR. Rather, the first three words in “You can have a copy of your personal data” are slightly underlined. When hovering over these words with the users’ mouse, a small box is displayed with a link to the settings.

154. Adding to the previous section, any means created by the controller for the exercise of rights should be easily accessible. This rule cannot be understated. An action by the controller as described above can be viewed only as an effort to hinder the exercise of rights by users, which infringes Article 12 (2) GDPR. Controllers, no matter their reasons, should not inhibit such a request. Upon closer examination by a supervisory authority in a specific case this could contribute to a breach of GDPR leading to sanctioning the controller.

#### ***Fickle – Inconsistent Interface (Annex I checklist 4.5.3)***

**Example 50:** The social media platform offers different versions (desktop, app, mobile browser). In each version, the settings (leading to access/objection etc.) are displayed with a different symbol, leaving users who switch between versions confused.

155. Confronted with interfaces across different devices that convey the same information through various visual signifiers, users are likely to take more time or have difficulties finding controls they know from one device to another. In the example above, this is due to the use of different symbols or icons to direct users to the settings. Confusing users in such a way could be considered conflicting with the facilitation of data subject rights as stated in Article 12 (2) GDPR.

#### ***Obstructing – Longer than necessary (Annex I checklist 4.4.2)***

156. Finally, any attempt to make the exercise of a right ***Longer than Necessary*** can be considered contrary to the GDPR.

**Example 51:** When users choose to delete the name and place of their high school or the reference to an event they attended and shared, a second window pops up asking to confirm that choice (“*Do you really want to do so? Why do you want to do this?*”).

157. Similarly to the amount of layers in a privacy policy (use case 2a) and the number of steps to reach or change a setting (use case 3b), the amount of steps or clicks users need to take to exercise a right should not be excessive. This of course depends on the complexity of operations conducted by the controller taking into consideration the specific context. It would however be unreasonable to require users to take a high number of unnecessary actions in order to finish exercising their right. For example, users should not be discouraged by additional questions, such as whether they really want to exercise this right or what the reasons for such a request are. In most cases they should be able to just exercise their right, without their motivation being put into question. Such practices, illustrated in the example above, can be considered contrary to Article 12 (2) GDPR as the controller hinders the exercise of the rights with unnecessary steps. This of course does not preclude the controller from receiving feedback by asking additional questions afterwards for the purpose of making the service better. By asking this question afterwards, answering it would depend solely on the users’ will and would not be mistaken for a requirement to exercise a right.

#### **d. Best practices**

**Exercise of the rights form:** to facilitate users in exercising their GDPR rights, provide a dedicated form that helps users understand their rights and that guides them carry out these kind of requests.

**Shortcuts:** see use case 1 for definition (p. 22) (e.g. *provide a link to account deletion in the user account*).

**Coherent wordings:** see use case 1 for definition (p. 22).

**Providing definitions:** see use case 1 for definition (p. 22).

**Use of examples:** see use case 1 for definition (p. 22).

**Sticky navigation:** see use case 2a for definition (p. 28).

**Explaining Consequences:** see use case 2c for definition (p. 32).

**Cross-device consistency:** see use case 3a for definition (p. 39).

**Data protection directory:** see use case 3b for definition (p. 45).

**Data protection controls relation:** see use case 3b for definition (p. 45).

### 3.5 So long and farewell: leaving a social media account

Use case 5: pausing the account/erasure of all personal data

#### a. Description of the context and relevant legal provisions

158. The end of the life cycle of an account describes the situation when users decide to leave the social network. In this situation, users usually decide to leave the social media platform permanently. However, there is often also the option of only temporarily disabling the account and pausing the service. The legal implications of both decisions differ and are described below.

##### i. Permanent erasure of the account

159. The decision to permanently leave the social media platform is accompanied by the right to erasure in Article 17 (1) (a) GDPR. In this context the word “deletion” is used more often than erasure.
160. The word “erasure” is not legally defined in Article 17 GDPR and is only mentioned as a form of processing in Article 4 (2) GDPR. Erasure can be generally understood as a (factual) impossibility to perceive the information about a data subject previously embodied in the data to be erased. After erasure, it must no longer be possible for anyone to perceive the information in question without disproportionate effort.
161. Anonymisation is another way of permanently removing the relation to a person. In other words, the use of anonymisation techniques is intended to ensure that the data subject can no longer be identified. Anonymisation also means that the principles of data protection law – such as the principle of purpose limitation – are no longer applicable (see Recital 26, phrases 4 and 5).
162. According to Article 12 (2) GDPR, the controller shall facilitate the exercise of data subject rights under Articles 15 to 22. According to this requirement, no substantive or formal hurdles may be created in the assertion of data subject rights. Therefore, if the exercise of the right of erasure is made more difficult without actual reason, this constitutes a violation of the GDPR. While there is a valid reason for social media providers objectively explain the consequences, such as deletion of all personal data, and ask data subjects to confirm this choice,<sup>73</sup> unnecessary hurdles also need to be avoided in this use case. From this follows e.g. that any grace period between users’ account deletion requests and the actual deletion of the account needs to be proportionate. Thus, such a time may not be excessive, taking into account necessary technical reasons for delays from immediate deletion, as well as a short time for users’ (re-)consideration about deleting their account once they have triggered the account deletion process. While users’ free will to change their mind needs to be respected, social media providers may not try to trigger such a change of mind by inciting users to come back, which would also constitute a hindrance of users’ right to deletion. During the grace period, the deletion process could be interrupted in some cases, e.g. when the user logs in again. If the deletion cannot be completed, the user must be informed and instructed on how to complete the deletion.
163. The decision to leave the social media platform triggers the consequences of erasure as stated in Article 17 (1) GDPR. If a data subject requests the deletion of the respective account, the controller of a social media platform needs to delete the data. Nevertheless, some data can remain with the social media platform for a certain period of time if Article 17 (3) GDPR is applicable. The exceptions listed in Article 17 (3) GDPR have to be interpreted narrowly and only apply in the cases explicitly named in this part of the provision. Any exception that a controller relies on under Article 17 (3) GDPR and the respective retention of data need to be justified by the controller, e. g., that national law requires the controller to store information related to the data subject for overriding reasons of public interest, for

---

<sup>73</sup> Contrary to the other data subject rights, see para. 154 above.

exercising the fundamental right of freedom of expression and information or for tax reasons. It goes without saying that such remaining data should only be stored internally by the Social Media Provider and should not be publicly visible for other users. In no way, however, does an exemption under Article 17 (3) GDPR enable the social media provider to keep running the account of the data subject longer than intended by the users after their request for deletion.

164. Independently of a request to delete the account, if users withdraw their consent under Article 7 (3) GDPR, processing of their consent-based provided data under Article 6 (1) (a) GDPR may no longer take place. In this case, other processing operations where the social media provider relies on other legal bases under Article 6 (1) GDPR may, under certain circumstances, still take place.
165. If users ask, however, to delete their account, no further processing should take place, irrespective of the underlying legal basis, unless one of the exceptions exhaustively listed in Article 17 (3) GDPR applies. In this context, it is important to keep in mind that retention is limited to the above-mentioned minimal storage
166. According to Article 25 (1) GDPR, the controller shall implement appropriate technical and organisational measures to put the data protection principles into practice. According to the Guidelines 04/2019 on Article 25 – Data Protection by Design and by Default, technical and organisational measures 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 should be suited to achieve the intended purpose, i.e. they must implement the data protection principles effectively. The requirement to appropriateness is thus closely related to the requirement of effectiveness.<sup>74</sup>

---

<sup>74</sup> Guidelines 04/2019 on Article 25 Data Protection by Design and by Default, page 6, para. 8.

## **ii. Pausing the account**

167. Alternatively, users are offered the opportunity to temporarily deactivate their account which allows users to leave the social media for a period of time without deleting their account permanently. In this case, the account is temporarily disabled and the profile, pictures, comments and reactions will be hidden until users reactivate their account, e. g. by logging back in. The main difference to the erasure is that the personal data remain with the social network and the account can be re-activated by users without a new registration.
168. Users starting the process to delete their account may find that the option to pause the account instead is pre-selected. While it might be useful for users who would not like to permanently delete their account just yet to be offered a pausing option, social media providers may not impose such cooling-off periods on users, especially through pre-selection. By offering the possibility of deactivation, the social media provider raises users' reasonable expectations that their personal data will not be processed in the same manner as during the active use of the account and that the social media provider reduces the processing of personal data to a strictly necessary level during this period. Users might expect that their data are not or not fully processed for specific purposes, e.g. by enhancing their profile with visits to third party websites that use appropriate targeting or tracking tools. In addition to informing users in a transparent manner about the consequences of pausing their account, any processing of data taking place during this pause needs to rely on a valid legal basis.
169. In respect of data processing relying on consent according to Article 6 (1) (a) GDPR, the social media provider must take into account that users expect that the consent they give during the registration or afterwards only covers data processing during their active use of the account. The EDPB recognises that the duration of consent depends on the context, the scope of the initial consent and the expectations of the data subject.<sup>75</sup> Although there is no specific time limit in the GDPR for how long consent will last, the validity will depend on the context, the scope of the original consent and the expectations of the data subject.<sup>76</sup> If the processing operations change or evolve considerably, then the original consent is no longer valid.<sup>77</sup> The EDPB recommends as a best practice that consent should be refreshed at appropriate intervals.<sup>78</sup> Providing all the information again helps to ensure that data subjects remain well informed about how their data is being used and how to exercise their rights.<sup>79</sup> If this is the case, consent needs to be obtained again<sup>80</sup> and all corresponding requirements must be fulfilled.
170. The reasonable expectations of the data subject should also be taken into consideration when Article 6 (1) (f) GDPR is applicable (see Recital 47). In particular, it is necessary to consider whether the data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may be taking place. However, users reasonably expect that only necessary data processing will take place during the time of deactivation. Moreover, the social media provider can only rely on legitimate interest if all steps of the legitimate interest test, including the balancing exercise are met. Any overriding interest or fundamental rights and freedoms of the data subject should be assessed on a case-by-case basis.

---

<sup>75</sup> Guidelines 5/2020 on consent, para 110.

<sup>76</sup> Guidelines 5/2020 on consent, para 110.

<sup>77</sup> Guidelines 5/2020 on consent, para 110.

<sup>78</sup> Guidelines 5/2020 on consent, para 111.

<sup>79</sup> Guidelines 5/2020 on consent, para 111.

<sup>80</sup> See Guidelines 5/2020 on consent, para 110.

171. Since contractual obligations are also suspended to a large extent during the deactivation, data processing operations are only necessary to a limited extent under Article 6 (1) (b) GDPR. Only the storage of users' data until the final decision on reactivation or deletion can be regarded as necessary.
172. In view of the fact that all previous data processing was aimed at an active account, additional information about the processing during the deactivation must be provided if it is not included in the general information under Articles 13, 14 GDPR. This follows from the principles of transparency and fairness under Article 5 (1) (a) GDPR and purpose limitation from Article 5 (1) (b) GDPR. The data processing following deactivation must be accompanied by sufficient information of the data subject. Therefore, the social media provider shall comprehensively inform users about the actual processing and its purposes during the pause and, if necessary, obtain new consent.

- b. Deceptive design patterns
  - i. Content-based patterns

***Overloading – Privacy Maze (Annex I checklist 4.1.2)***

173. In this use case, the deceptive design pattern ***Privacy maze*** occurs when users are buried under a mass of information, spread across several places, to keep them from deleting their account, as the example below shows. While some additional information before this step is quite desirable, such as the indication that users have access to their data before deletion, general unrelated information is no longer crucial. Users should not be unnecessarily delayed in taking this step.

**Example 52:** Users are looking for the right to erasure. They have to call up the account settings, open a sub-menu called "privacy", and have to scroll all the way down to find a link to delete the account.

***Stirring – Emotional Steering (Annex I checklist 4.3.1)***

**Example 53:** On the first information level, information is given to users highlighting only the negative, discouraging consequences of deleting their accounts (e.g. "*you'll lose everything forever*" or "*your friends will forget you*").

174. Whereas regret over the termination of contractual relationship appears socially adequate and is therefore difficult to capture in legal terms, a comprehensive description of the supposedly negative consequences caused by users erasing their account constitutes an impediment against their decision if done as in the example above which plays with the fear of missing out (FOMO), making the choice of deleting one's account look like particularly punishing. Such ***Emotional steering***, threatening users that they will be left alone if they delete their account, constitutes an infringement of the obligation to facilitate the exercise of data subject rights under Article 12 (2) GDPR, as well as of the principle of fairness under Article 5 (1) (a) GDPR.

***Left in the dark – Ambiguous wording or information (Annex I checklist 4.6.3)***

175. In the context of deleting a social media account, users can also be confronted with the deceptive design pattern ***Ambiguous wording or information***, as shown in the following example.

**Example 54:** When users delete their account, they are not informed about the time their data will be kept once the account is deleted. Even worse, at no point in the whole deletion

process users are advised about the fact that “*some of the personal data*” might be stored even after deleting an account. They need to look for the information by themselves, across the different information sources available.

**Example 55:** Users can only delete their account through links named “See you” or “Deactivate” available in their account.

176. In these examples, the wording used for the links does not clearly convey the fact that users will be redirected to the account deletion process. Instead, users are likely to think of other functionalities such as logging off until the next use, or deactivation of their account. As such, this could be interpreted as an infringement of Article 12 (2) GDPR stating that data controllers should facilitate the exercise of the rights of data subjects. By creating confusion on the expectations of users associated with the link, the social media platform does not fully facilitate the exercise of the right of erasure. The use of such equivocal words in other context could infringe GDPR provisions such as Article 7 GDPR and by extension Article 17 (1) (b) GDPR.

## ii. Interface-based patterns

### *Skipping – Deceptive snugness (Annex I checklist 4.2.1)*

**Example 56:** In the process of deleting their account, users are provided with two options to choose from: To delete their account or to pause it. By default, the pausing option is selected.

177. The first option of deleting the account results in the deletion of all personal data of users, meaning that the social media platform is no longer in possession of these data, except for data under the temporary exception of Article 17 (3) GDPR. In contrast, with the second option of pausing the account, all personal data are kept and potentially processed by the social media provider. This necessarily poses more risks to the data subject, for example if a data breach happens and data still stored by the social media provider are accessed, duplicated, transferred or otherwise processed. The default selection of the pause option is likely to nudge users to select it instead of deleting their account as initially intended. Therefore, the practice described in this example can be considered as an infringement of Article 12 (2) GDPR since it does not, in this case, facilitate the exercise of the right to erasure, and even tries to nudge users away from exercising it.

### *Skipping – Look over there (Annex I checklist 4.2.2)*

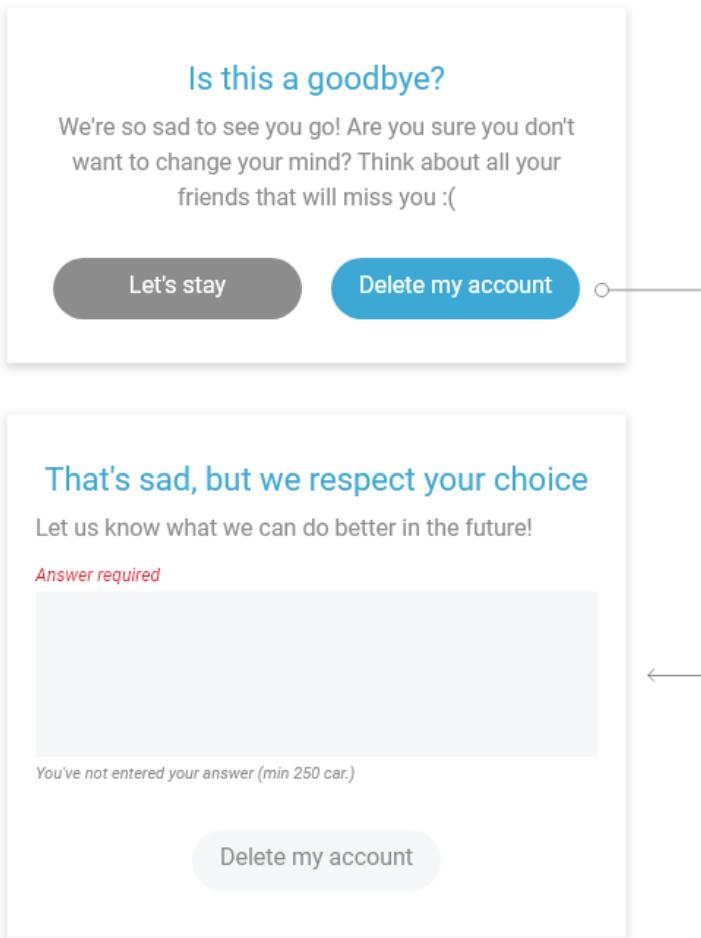
178. Providing users with a mean to download their data when they indicate their will to delete their account can be a relevant option to offer. Indeed, once their account is deleted, their personal data will be erased after a certain period of time. This means that, if they do not get a copy of their personal data, they will entirely lose them. However, the presentation of this option can constitute a **Look over there** deceptive design pattern, as shown in the following example.

**Example 57:** After clicking on “Delete my account”, users are presented with the option to download their data, implemented as the right to portability, before deleting the account. When clicking to download their information, users are redirected on a download information page. However, once users have chosen what and how to download their data, they are not redirected to the deletion process.

179. In the example above, it could be considered that the way the download option is implemented does not facilitate the exercise of the right to erasure associated with the account's deletion. Indeed, once users have downloaded their data, they are not brought back to the deletion process. To go back to it, they will have to click several times. Hindering in such a way the exercise of a right infringes Article 12 (2) GDPR. Furthermore, providing a mean to easily reach the deletion process after downloading one's data is a simple feature to implement. In that regard, it could be considered that the obligation to implement appropriate technical and organisational measures in Article 25 (1) GDPR is not respected as users are not able to continue to exercise their rights effectively.

***Obstructing – Longer than necessary (Annex I checklist 4.4.2)***

180. As detailed in use case 4, any irrelevant steps added to the exercise of a right might contravene provisions of the GDPR, in particular Article 12 (2). This applies to the moment where users aim to delete their account, as it would interfere with the right to erasure associated with such a request.



**Example 58:** In this example, users first see a confirmation box to erase their account after having clicked on the corresponding link or button in their account. Even though there is some **Emotional Steering** in this box, this step can be seen as a security measure in order for users not to delete their account following a mis-click in their account. However, when users click on the “Delete my account” button, they are confronted with a second box asking them

to textually describe the reason they want to leave the account. As long as they have not entered something in the box, they cannot delete their account as the button associated with the action is inactive and greyed out. This practice makes the erasure of an account **Longer than Necessary**, especially as asking users to produce a text describing why they want to leave an account requires extra effort and time and should not be mandatory to delete one's account.

181. As noted previously, when exercising a right, users should not have to answer questions not related to the exercise of the right itself. Having to justify one's choice or explain how the social media platform should improve does not fall under that category. In the illustrated example, this issue is heightened as data subjects have to write an answer instead of selecting a pre-made proposition in a list, which is even more burdensome for them since it requires to fully create the answer. Such mechanism could exclude some users from exercising their right altogether if they are not comfortable enough to write down an answer.
182. However, this does not mean that a list of pre-made answers is an acceptable step to add to the process of deleting one's account. This is especially true if these answers are associated with further steps and actions imposed on users, as the example below shows.

**Example 59:** The social media provider makes it mandatory for users to answer a question about their reasons for wishing to erase their account, through a selection of answers from a drop-down menu. It appears to users that answering this question (apparently) enables them to achieve the action they want, i.e. to delete the account. Once an answer is selected, a pop-up window appears, showing users a way of solving the issue stated in their answer. The question-answer process therefore slows down users in their account erasure process.

183. In addition to making the erasure of the account particularly lengthy, a **Look Over There** mechanism aims to divert users away from deleting their account by providing a solution to their motivation behind leaving the social media platform. These hinder the exercise of the right to erasure and, by extension, discourage the data subjects to exercise their right.

#### **Fickle – Decontextualising (Annex I checklist 4.5.2)**

184. Finally, the **Decontextualising** deceptive design pattern can also be found when users wish to delete their account.

**Example 60:** On the social media platform XY, the link to deactivate or delete the account is found in the “Your XY Data” tab.

185. In general, the terms used to title a page or section of the social media platform dedicated to data protection matters should clearly reflect the kind of information or control included there. Average users are unlikely to link actions to delete or deactivate their account to data management. In the previous example, users would not expect the functionality for deleting their account in a page called “Your XY Information” that alludes to seeing and potentially reviewing one's information. Instead, they would look for a “General” page or a “Delete my account” page. Therefore, from the view point of users, the options are placed in a setting that it is out of context and does not match user expectations.

**Example 61:** The actual tab to erase an account is found in the section “*delete a function of your account*”.

186. In this example, users could mistakenly understand the section title as the mere place where to adjust single functions. Users would therefore not expect the option to delete the whole account to be there. That makes it hard for users to find the correct link to erase the entire account.
187. The ***Decontextualising*** deceptive design pattern, as illustrated in the two examples above, could be considered a breach of Article 12 (2) GDPR, given that users would have difficulties to find the right place where to exercise their right to erasure.

### c. Best Practices

**Coherent wordings:** see use case 1 for definition (p.22).

**Providing definitions:** see use case 1 for definition (p.22).

**Use of examples:** see use case 1 for definition (p.22).

**Explaining Consequences:** see use case 2c for definition (p.32).

**Cross-device consistency:** see use case 3a for definition (p.39).

For the European Data Protection Board

The Chair

(Andrea Jelinek)

## 4 ANNEX I: LIST OF DECEPTIVE DESIGN PATTERN CATEGORIES AND TYPES

The following list provides an overview of deceptive design pattern categories and the types of deceptive design patterns within each category. It also lists the GDPR provisions most concerned by the deceptive design pattern types. Readers should keep in mind that, as mentioned above, the principle of fair processing laid down in Article 5 (1) (a) GDPR is a starting point for an assessment of existence of deceptive design patterns. It has an umbrella function and all deceptive design patterns would not comply with it irrespectively of compliance with other data protection principles.<sup>81</sup>

For each pattern, the list also contains the numbers of examples and corresponding use case (UC) to help readers find them quickly.

It is important to note that this list is not exhaustive and that deceptive design patterns can therefore also occur in use cases that do not contain an example for this deceptive design pattern type in the text of the Guidelines.

### 4.1 Overloading

Burying users under mass of requests, information, options or possibilities in order to deter them from going further and make them keep or accept certain data practice.

#### 4.1.1 Continuous prompting<sup>82</sup>

Pushing users to provide more personal data than necessary for the purpose of processing or to agree with another use of their data by repeatedly asking users to provide data or to consent to a new purpose of processing. Such repetitive prompts can happen through one or several devices. Users are likely to end up giving in, wearied from having to refuse the request each time they use the platform which disrupts them in their use.

##### **Concerned GDPR provisions:**

- *Purpose limitation: Article 5 (1) (b);*
- *Freely given consent: Article 7 in conjunction with Article 4 (11);*
- *Specific consent: Article 7 (2).*

**Examples:** UC 1 examples 1, 2; UC 3a example 34 (illustration).

#### 4.1.2 Privacy Maze

When users wish to obtain certain information or use a specific control or exercise a data subject right, it is particularly difficult for them to find it as they have to navigate through too many pages in order to obtain the relevant information or control, without having a comprehensive and exhaustive overview available. Users are likely to give up or miss the relevant information or control.

##### **Concerned GDPR provisions:**

---

<sup>81</sup> See above, para. 9 of these Guidelines.

<sup>82</sup> This pattern is closely related to a type of pattern called “Nagging” found in the academic literature.

- *Principle of transparency: Article 5 (1) (a) and transparent information: Article 12 (1);*
- *Principle of fairness: Article 5 (1) (a);*
- *Easily accessible information: Article 12 (1);*
- *Easy access to rights: Article 12 (2);*
- *Informed consent: Article 7 in conjunction with Article 4 (11).*

**Examples:** UC 2a example 17; UC 3a example 33; UC 3b example 37; UC 4 examples 47 (illustration) and 48 (illustration); UC 5 example 51.

#### 4.1.3 Too many options

Providing users with (too) many options to choose from. The amount of choices leaves users unable to make any choice or make them overlook some settings, especially if information is not available. It can lead them to finally give up or miss the settings of their data protection preferences or rights.

##### **Concerned GDPR provisions:**

- *Principles of transparency and fairness: Article 5 (1) a;*
- *Transparent information: Article 12 (1).*

**Example:** UC 3b example 35.

## 4.2 Skipping

Designing the interface or user journey in such a way that users forget or do not think about all or some of the data protection aspects.

#### 4.2.1 Deceptive snugness

By default, the most data invasive features and options are enabled. Relying on the default effect which nudges individuals to keep a pre-selected option, users are unlikely to change this even if given the possibility.

##### **Concerned GDPR provisions:**

- *Data protection by design and by default: Article 25 (1);*
- *Consent: Articles 4 (11) and 6 (illegal practice to activate a processing based on consent by default).*

**Examples:** UC 1 example 9; UC 3b examples 39 and 40 (illustration); UC 5 example 55.

#### 4.2.2 Look over there

A data protection related action or information is put in competition with another element which can either be related to data protection or not. When users choose this distracting option, they are likely to forget about the other, even if it was their primary intent.

##### **Concerned GDPR provisions:**

- *Principles of transparency and fairness*: Article 5 (1) a;
- *Transparent information*: Article 12 (1);
- *Exercise of rights*: Article 12 (2).

**Examples:** UC 2c example 25; UC 3a example 29; UC 5 examples 56 and 58.

#### 4.3 Stirring

Affecting the choice users would make by appealing to their emotions or using visual nudges.

##### 4.3.1 Emotional Steering<sup>83</sup>

Using wording or visual elements (such as style, colours, pictures or others) in a way that confers the information to users in either a highly positive outlook, making users feel good, safe or rewarded, or in a highly negative one, making users feel scared, guilty or punished. Influencing the emotional state of users in such a way is likely to lead them to make an action that works against their data protection interests.

##### Concerned GDPR provisions:

- *Principles of transparency and fairness*: Article 5 (1) a;
- *Transparent information*: Article 12 (1);
- *Exercise of rights*: Article 12 (2);
- *Child's consent*: Article 8;
- *Informed consent*: Article 7 in conjunction with Article 4 (11);

**Examples:** UC1 examples 4, 5, 6; UC 5 example 52.

##### 4.3.2 Hidden in plain sight

Use a visual style or technique for information or data protection controls that nudges users toward less restrictive and thus more invasive options.

##### Concerned GDPR provisions:

- *Principle of fairness*: Article 5 (1) a;
- *Freely given consent*: Article 7 in conjunction with Article 4(11);
- *Clear information*: Article 12 (1);
- *Exercise of rights*: Article 12 (2)

**Examples:** UC1 example 8, UC 3a example 34 (illustration); UC 3b example 40 (illustration); UC 4 example 48.

---

<sup>83</sup> This pattern is closely related to a type of pattern called “*Toying with Emotions*” found, inter alia, in reports of intergovernmental organisations such as European Commission, Directorate-General for Justice and Consumers, Lupiáñez-Villanueva, F., Boluda, A., Bogliacino, F., et al., *Behavioural study on unfair commercial practices in the digital environment : dark patterns and manipulative personalisation : final report*, Publications Office of the European Union, 2022, <https://data.europa.eu/doi/10.2838/859030> and OECD (2022), “Dark commercial patterns”, *Documents de travail de l'OCDE sur l'économie numérique*, n° 336, Éditions OCDE, Paris, <https://doi.org/10.1787/44f5e846-en>.

## 4.4 Obstructing<sup>84</sup>

Hindering or blocking users in their process of obtaining information or managing their data by making the action hard or impossible to achieve.

### 4.4.1 Dead end

While users are looking for information or a control, they end up not finding it as a redirection link is either not working or not available at all. Users are left unable to achieve that task.

#### **Concerned GDPR provisions:**

- *Easily accessible information*: Article 12 (1);
- *Exercise of rights*: Article 12 (2);
- *Data protection by design and by default*: Article 25 (1).

**Examples:** UC1 examples 10, 11; UC 2a example 18; UC 3a examples 30, 31; UC 4 example 43.

### 4.4.2 Longer than necessary

When users try to activate a control related to data protection, the user journey is made in a way that requires more steps from users, than the number of steps necessary for the activation of data invasive options. This is likely to discourage them from activating such control.

#### **Concerned GDPR provisions:**

- *Easily accessible information*: Article 12 (1);
- *Exercise of rights*: Article 12 (2);
- *Right to object*: Article 21 (1);
- *Consent withdrawal*: Article 7 (3);
- *Data protection by design (and by default)*: Article 25 (1).

**Examples:** UC 1 example 7; UC 3a example 32; UC 4 example 50; UC 5 examples 57 (illustration) and 58.

### 4.4.3 Misleading action

A discrepancy between information and actions available to users nudges them to do something they do not intend to. The difference between what users expect and what they get is likely to discourage them from going further.

#### **Concerned GDPR provisions:**

- *Transparent information*: Article 12 (1);
- *Fairness of processing*: Article 5 (1) (a).

---

<sup>84</sup> This category is closely related to the strategy called “Obstruction” defined and described in Gray Colin M., Kou Yubo, Battles Bryan, Hoggatt Joseph, and Toombs Austin L. 2018. The Dark (Patterns) Side of UX Design. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (Montreal QC, Canada) (CHI ’18). ACM, New York, NY, USA, Article 534, 14 pages. <https://doi.org/10.1145/3173574.3174108>.

- *Informed consent*: Article 7 (2) in conjunction with Article 4 (11).

**Examples:** UC 1 example 3; UC 3a example 28.

## 4.5 Fickle

The design of the interface is unstable and inconsistent, making it hard for users to figure out the nature of the processing, to properly make a choice concerning their data, and to find where the different controls are.

### 4.5.1 Lacking hierarchy

Information related to data protection lacks hierarchy, making information appear several times and being presented in several ways. Users are likely to be confused by this redundancy and to be left unable to fully understand how their data are processed and how to exercise control over them.

**Concerned GDPR provisions:**

- *Easily accessible information*: Article 12 (1);
- *Exercise of the rights*: Article 12 (2).

**Examples:** UC 2a examples 13 and 14.

### 4.5.2 Decontextualising

A data protection information or control is located on a page that is out of context. Users are unlikely to find the information or control as it would not be intuitive to look for it on this specific page.

**Concerned GDPR provisions:**

- *Easily accessible information*: Article 12 (1);
- *Transparent information*: Article 12 (1);
- *Exercise of the rights*: Article 12 (2).

**Examples:** UC 3b examples 41, 42; UC 5 examples 59 and 60.

### 4.5.3 Inconsistent interface

An interface is not consistent across different contexts (e.g., a data protection related menu does not display the same items on mobile and on desktop) or with users' expectations (e.g., an option whose location has been switched with that of another option). These differences can lead users not to find the desired control or information or to interact with an element of the interface out of habits even though this interaction leads to make a data protection choice users do not want.

**Concerned GDPR provisions:**

- *Easily accessible information*: Article 12 (1);

- *Exercise of the rights: Article 12 (2).*

**Examples:** UC 3b example 39; UC 4 example 50.

#### 4.5.4 Language discontinuity

Information related to data protection is not provided in the official language(s) of the country where users live, whereas the service is. If users do not master the language in which data protection information is given, they will not be able to easily read it and therefore likely to not be aware of how data are processed.

##### **Concerned GDPR provisions:**

- *Fairness of processing: Article 5 (1) (a);*
- *Intelligible information: Article 12 (1), Article 13 and Article 14;*
- *Use of clear and plain language for the information: Article 12 (1), Article 13 and Article 14.*

**Examples:** UC 2a example 16; UC 3a examples 26 (illustration) and 27; UC 4 example 44.

### 4.6 Left in the dark

The interface is designed in a way to hide information or controls related to data protection or to leave users unsure of how data is processed and what kind of controls they might have over it.

#### 4.6.1 Conflicting information

Giving pieces of information to users that conflict with each other in some way. Users are likely to be left unsure of what they should do and about the consequences of their actions, therefore likely not to take any and to just keep the default settings.

##### **Concerned GDPR provisions:**

- *Fairness of processing: Article 5 (1) (a);*
- *Transparent information: Article 12 (1);*
- *Informed consent: Article 7 (2) in conjunction with Article 4 (11).*

**Examples:** UC 2a example 12; UC 2c example 20; UC 3b example 36.

#### 4.6.2 Ambiguous wording or information

Using ambiguous and vague terms when giving information to users. They are likely to be left unsure of how data will be processed or how to exercise control over their personal data.

##### **Concerned GDPR provisions:**

- *Fairness of processing: Article 5 (1) (a);*
- *Transparent information: Article 12 (1);*
- *Use of clear and plain language for the information: Article 12 (1);*

- *Informed consent*: Article 7 (2) in conjunction with Article 4 (11);
- *Incomplete information*: Article 13
- *Specific provisions depending on the particular use case, for example Article 34 for UC 2c.*

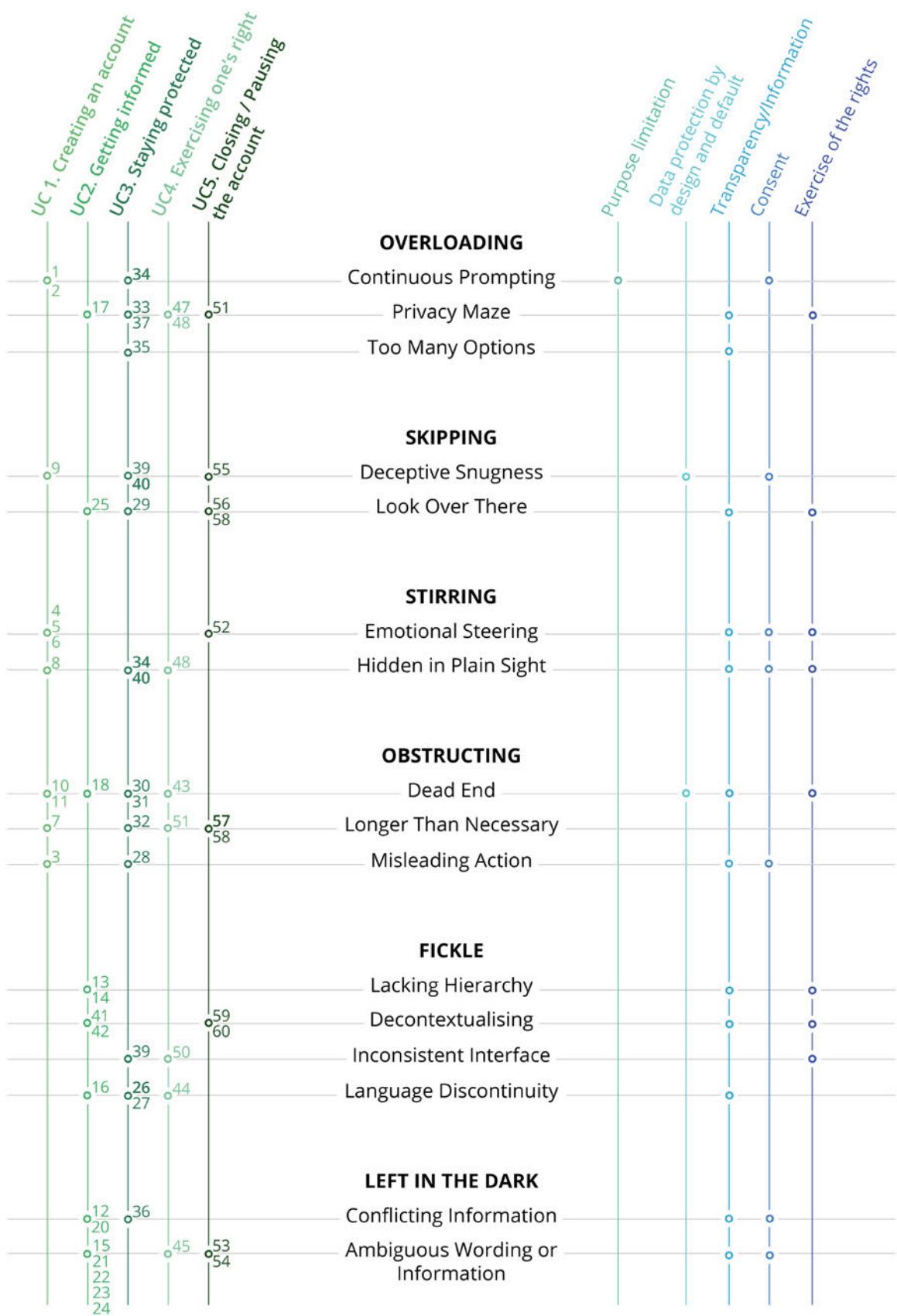
**Examples:** UC 2a example 15; UC 2c examples 21, 22, 23, 24; UC 4 example 45; UC 5 examples 53 and 54.

## LIFECYCLE

# DECEPTIVE DESIGN OVERVIEW

## GDPR PROVISIONS

All deceptive design go against the fairness principle



## 5 ANNEX II: BEST PRACTICES

The following list provides an overview of best practices described in the Guidelines at the end of each use case. These can be used to design user interfaces which facilitate the effective implementation of the GDPR. Such best practices can offer a first step toward a standardised way for users to effectively control their data and exercise their rights.

**Shortcuts:** Links to information, actions or settings that can be of practical help to users to manage their data and their data protection settings should be available wherever they are confronted to related information or experience (*e.g. links redirecting to the relevant parts of the privacy policy; e.g. in the privacy policy, provide for each data protection information links that directly redirects to the related data protection pages on the social media platform; provide users with a link to reset their password; when users are informed about an aspect of the processing, they are invited to set their related data preferences on the corresponding setting/dashboard page; provide a link to account deletion in the user account*).

**Bulk options:** Putting options that have the same processing purpose together, so that users can change them more easily, while still leaving users the possibility to make more granular changes. If social media platforms present bulk options, these should not contain unexpected or unrelated elements (for example elements with different purposes). If the processing require consent, the bulk options must be in line with the EDPB Guidelines on consent, especially para. 42-44.

**Contact information:** The company contact address for addressing data protection requests should be clearly stated in the privacy policy. It should be present in a section where users can expect to find it, such as a section on the identity of the data controller, a rights related section or a contact section.

**Reaching the supervisory authority:** Stating the specific identity of the supervisory authority and including a link to its website or the specific website page related to lodging a complaint. This information should be present in a section where users can expect to find it, such as a rights related section.

**Privacy Policy Overview:** At the start / top of the privacy policy, include a (collapsible) table of contents with headings and sub-headings that shows the different passages the privacy notice contains. The names of the single passages clearly lead users regarding the exact content and allow them to quickly identify and jump to the section they are looking for.

**Change spotting and comparison:** When changes are made to the privacy notice, make previous versions accessible with date of release and highlight changes.

**Coherent wordings:** Across the website, the same wording and definition is used for the same data protection. The wording used in the privacy policy should match the one used on the rest of the platform.

**Providing definitions:** When using unfamiliar or technical words or jargon, providing a definition in plain language will help users understand the information provided to them. The definition can be given directly into the text, when users hover over the word, as well as be made available in a glossary.

**Contrasting Data protection elements:** Making data protection related elements or actions visually striking in an interface that is not directly dedicated to the matter. For example, when posting a public

message on the platform, controls over association of the geolocation should be directly available and clearly visible.

**Data Protection Onboarding:** Just after the creation of an account, include data protection points within the onboarding experience of the social media provider for users to smoothly discover and set their preferences. For example, this can be done by inviting them to set their data protection preferences after adding their first friend or sharing their first post.

**Use of examples:** In addition to mandatory information clearly and precisely stating the purpose of processing, examples can be used to illustrate a specific data processing to make it more tangible for users.

**Sticky navigation:** While consulting a page related to data protection, the table of contents can be constantly displayed on the screen allowing users to always situate themselves on the page and to quickly navigate in the content thanks to anchor links.

**Back to top:** Include a return to top button at the bottom of the page or as a sticky element at the bottom of the window to facilitate users' navigation on a page.

**Notifications:** Notifications can be used to raise awareness of users on aspects, change or risks related to personal data processing (e.g. *when a data breach occurred*). These notifications can be implemented in several ways, such as through inbox messages, pop-in windows, fixed banners at the top of the webpage, etc.

**Explaining consequences:** When users want to activate or deactivate a data protection control, or give or withdraw their consent, inform them in a neutral way on the consequences of such action.

**Cross-device consistency:** When the social media platform is available through different devices (e.g. computer, smartphones, etc.), settings and information related to data protection should be located in the same spaces across the different versions and should be accessible through the same journey and interface elements (menu, icons, etc.).

**Data protection directory:** For easy orientation through the different section of the menu, provide users with an easily accessible page from where all data protection related actions and information are accessible. This page could be found in the social media provider main navigation menu, the user account, through the privacy policy, etc.

**Contextual information:** in addition to an exhaustive privacy policy, bring short bits of information at the most appropriate time for the user to have a specific and continuous information on how their data are processed.

**Self-explanatory URL:** pages related to data protection settings or information should use a web address that clearly reflects their content. For example, a page centralising data protection control could have a URL such as [social-network.com]/data-settings.

**Exercise of the rights form:** to facilitate users in exercising their GDPR rights, provide a dedicated form that helps users understand their rights and that guides them carry out these kind of requests.

# Request for mandate



EDPB Plenary meeting, 07 April 2020

## **07/04/2020 - Request for mandate regarding geolocation and other tracing tools in the context of the COVID-19 outbreak - Technology ESG**

### **Background**

Following the remote plenary meeting on 3 April 2020, the EDPB decided to provide guidance on data protection issues arising in the context of the COVID-19 crisis. Guidance on the issues relating to data protection and the use of tracking and geolocation tools in the context of the COVID-19 outbreak was identified as a priority.

### **Description of the content of the mandate**

Therefore, the TECH ESG is asked to focus in particular on the following issues:

- the use of aggregated / anonymised location data (e.g. provided by telecom or information society service providers) and the effectiveness of aggregation and anonymization techniques;
- the application of the principles of lawfulness, necessity, proportionality, including accuracy, and data minimisation to the different means available to gather location data or trace interactions between data subjects;
- general legal analysis of the use of apps and collection of personal data by apps to help contain the spread of the virus;
- the required safeguards to ensure the respect of data protection principles, including with regard to data retention, in the context of using geo-location or other tracing tools.
- the identification of recommendations or functional requirements for contact tracing applications ;
- the necessity to subject the measures taken to a pre-defined timeframe limited to what is strictly necessary to tackle the emergency situation;

### **Request to the Plenary:**

The Plenary is requested to give a mandate to the TECH ESG that will work according to the above-mentioned content. It shall liaise with the CEH and KEYP ESGs whenever necessary.

# Opinion of the Board (Art. 64)



## **Opinion 27/2020 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of Coloplast Group**

**Adopted on 8 December 2020**

## Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT .....	5
3	CONCLUSIONS / RECOMMENDATIONS.....	5
4	FINAL REMARKS.....	5

## **The European Data Protection Board**

Having regard to Article 63, Article 64(1)(f) and Article 47 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 European Economic Area (hereinafter “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 Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “EDPB”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “SA”) aims to approve binding corporate rules (hereinafter “BCRs”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s (BCRs Lead) draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA, in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party<sup>2</sup>, endorsed by the EDPB.

---

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

<sup>2</sup> The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

(4) This opinion only covers EDPB's consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP256 rev01 of the Article 29 Working Party, as endorsed by the EDPB<sup>3</sup>. Accordingly, this opinion and the SAs' review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR.

(5) WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for controllers (hereinafter "BCR-C"), including the Intra-Company Agreement where applicable, and the application form. WP264 of the Article 29 Working Party, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev01. Additionally, WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs' national laws. The EDPB is subject to Regulation 1049/2001<sup>4</sup> pursuant to Article 76(2) GDPR.

(6) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data<sup>5</sup>.

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

## **HAS ADOPTED THE FOLLOWING OPINION:**

### **1 SUMMARY OF THE FACTS**

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of Coloplast Group were reviewed by the Danish Supervisory Authority (Datatilsynet) as the BCR lead supervisory authority (hereinafter the "BCR Lead SA").
2. The BCR Lead SA has submitted its draft decision regarding the draft BCR-C of Coloplast Group requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 16 September 2020. The decision on the completeness of the file was taken on 9 October 2020.

---

<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, WP 256 rev.01.

<sup>4</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.

<sup>5</sup> This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

## 2 ASSESSMENT

3. The draft BCR-C of Coloplast Group applies to all Coloplast Entities, including those entities established in the EEA or in a country with an adequate level of data protection as recognised by a decision of the EC and those entities established outside the EEA. With regard to Coloplast Entities outside the EEA, the BCR-C applies to personal data transferred directly or indirectly from the EU.
4. Concerned data subjects include employees, customers, subcontractors and other third parties processed internally by the Coloplast Entities as part of their regular business activities.
5. The draft BCR-C of Coloplast Group have been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the Coloplast Group draft BCRs-C contain all elements required under Article 47 GDPR and WP256 rev01, in concordance with the draft decision of the BCR Lead SA submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

## 3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the Coloplast Group Intra-Group Agreement, the EDPB considers that the draft decision of the BCR Lead SA may be adopted as it is, since the draft BCR-C of Coloplast Group contain appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data will be transferred to and processed by the group members based in third countries. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

## 4 FINAL REMARKS

7. This opinion is addressed to the BCR Lead SA and will be made public pursuant to Article 64(5)(b) GDPR.
8. According to Article 64(7) and (8) GDPR, the BCR Lead SA shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
9. Pursuant to Article 70(1)(y) GDPR, the BCR Lead SA shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.
10. In accordance with the judgment of the Court of Justice of the European Union C-311/18<sup>6</sup>, it is the responsibility of the data exporter in a Member State, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter in a Member State, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

---

<sup>6</sup> CJEU, *Data Protection Commissioner v .Facebook Ireland Ltd and Maximillian Schrems*, 16 July 2020, C-311/18.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

# 2021 ANNUAL REPORT

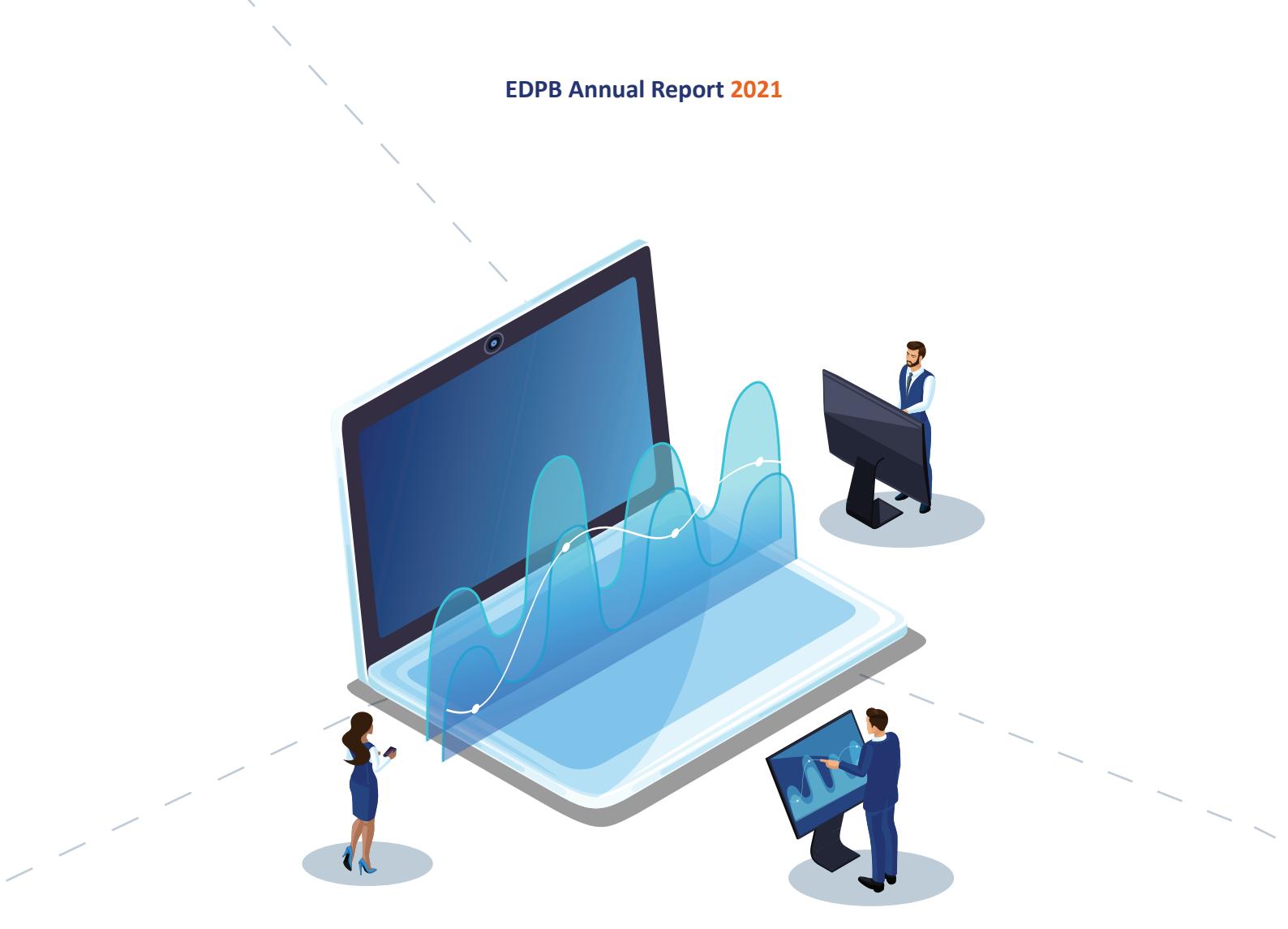
Enhancing the depth  
and breadth of  
data protection

## EXECUTIVE SUMMARY



# ENHANCING THE DEPTH AND BREADTH OF DATA PROTECTION EXECUTIVE SUMMARY

Further details about the EDPB can be found on our website at [edpb.europa.eu](http://edpb.europa.eu).



The European Data Protection Board (EDPB) is an independent European body, established by the [General Data Protection Regulation \(GDPR\)](#), which aims to ensure the consistent application of data protection rules across the European Economic Area (EEA). It achieves this aim by promoting cooperation between national Supervisory Authorities (SAs) and issuing general, EEA-wide guidance regarding the interpretation and application of data protection rules.

The EDPB comprises the Heads of the EU SAs and the European Data Protection Supervisor (EDPS). The SAs of the EEA countries (Iceland, Liechtenstein and Norway) are also members of the EDPB, although they do not have the right to vote. The European Commission and – with regard to GDPR-related matters – the European Free Trade Association

Surveillance Authority have the right to participate in the activities and meetings of the EDPB. The EDPB is based in Brussels.

The EDPB has a Secretariat, which is provided by the EDPS. A [Memorandum of Understanding](#) determines the terms of cooperation between the EDPB and the EDPS.

## **1. 2021 – HIGHLIGHTS**

### **1.1. GUIDANCE FOLLOWING THE SCHREMS II RULING**

As part of its guidance work following the Case C-311/18 *Schrems II* ruling by the Court of Justice of the European Union, the EDPB issued recommendations and a joint opinion with the EDPS. The updated Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data following public consultation complement and are consistent with the European Commission's Standard Contractual Clauses (SCCs) for international data transfers. The EDPS-EDPB Joint Opinion 02/2021 on SCCs for the transfer of personal data to third countries guides exporters on how to apply the SCCs correctly by taking into account the new requirements under the GDPR and the *Schrems II* ruling.

### **1.2. EDPB-EDPS JOINT OPINION ON THE ARTIFICIAL INTELLIGENCE ACT**

Following the publication of the European Commission's Proposal for a Regulation laying down harmonised rules on artificial intelligence (AI), the EDPB and the EDPS adopted the Joint Opinion 05/2021 on the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). The joint opinion covers points regarding the proposal's scope, risk-based approach and alignment with the GDPR, but also prohibited uses of AI, high-risk AI systems, governance and European AI Board, regulatory sandboxes and interaction with the data protection framework.

### **1.3. ART. 65 GDPR BINDING DECISION ON WHATSAPP IRELAND**

The EDPB adopted a binding decision based on Art. 65(1)(a) GDPR, which sought to address the lack of consensus on certain aspects of a draft decision issued by the Irish SA as lead supervisory authority (LSA) regarding WhatsApp Ireland Ltd. (WhatsApp IE) and the subsequent objections expressed by a number of concerned supervisory authorities (CSAs). The EDPB concluded that the Irish SA should amend its draft decision on WhatsApp IE regarding infringements of transparency, the period to bring processing operations into compliance and the calculation of the fine.

### **1.4. FIRST URGENT BINDING DECISION UNDER ART. 66 GDPR**

The EDPB adopted its first urgent binding decision under Art. 66(2) GDPR following a request from the Hamburg SA, which had adopted provisional measures against Facebook Ireland Ltd. (Facebook IE) under Art. 66(1) GDPR. The provisional measures prohibited Facebook IE from processing, for three months, the data of German residents using WhatsApp for Facebook IE's own purposes, following a change in the Terms of Service and Privacy Policy applicable to European users of WhatsApp IE.

The EDPB decided that the conditions to prove the existence of an infringement to the GDPR and the urgency to adopt final measures were not met, hence stating that the Irish SA did not need to adopt final measures against Facebook IE. The EDPB, however requested the Irish SA to perform, as a matter of priority, a statutory investigation; to determine whether such processing activities were taking place or not and, if they were, whether they had a proper legal basis under Art. 5(1)(a) and Art. 6(1) GDPR; and to further investigate the role of Facebook IE.

### 1.5. EDPB OPINIONS ON DRAFT UK ADEQUACY DECISIONS

In 2021, the EDPB issued two opinions on the European Commission draft Implementing Decisions on the adequate protection of personal data in the UK and recommendations on the adequacy referential under the Law Enforcement Directive (LED).

Opinion 14/2021 relates to the adequate protection of personal data in the UK pursuant to the GDPR. It assesses general data protection aspects of the UK legal framework. The opinion also examines the UK public authorities' access to personal data transferred from the EEA to the UK, for the purposes of law enforcement and national security. Opinion 15/2021 also relates to the adequate protection of personal data in the UK but is based on the LED. It analyses the draft adequacy decision in the light of Recommendations 01/2021, as well as the relevant case law reflected in Recommendations 02/2020 on the European Essential Guarantees for surveillance measures. This was the first draft implementing decision on a third country's adequacy under the LED ever presented by the European Commission and assessed by the EDPB. Recommendations 01/2021 on the adequacy referential under the LED provide guidance to the European Commission on the level of data protection in third countries and international organisations under the LED.

### 2. EUROPEAN DATA PROTECTION BOARD ACTIVITIES IN 2021

To ensure the consistent application of the GDPR across the EEA, the EDPB issues general guidance to clarify European data protection laws. In 2021, the EDPB adopted 14 [guidelines](#) and [recommendations](#) on topics such as data breach notifications, codes of conduct as data transfer tools, storing credit card data, virtual voice assistants and the meaning of

specific terms in the GDPR. Amongst those guidelines and recommendations, the EDPB also adopted six documents after public consultation.

The EDPB also adopted 15 [legislative consultations](#) or [statements](#) addressed to the EU legislator or Member States.

The EDPB issued consistency opinions to ensure the consistent application of the GDPR by national SAs. In 2021, they issued 35 [opinions](#) under Art. 64 GDPR. These opinions mainly concerned draft decisions regarding Binding Corporate Rules, draft accreditation requirements for a code of conduct monitoring body or a certification body, as well as draft Standard Contractual Clauses.

### 3. SUPERVISORY AUTHORITY ACTIVITIES IN 2021

National SAs are independent public authorities that ensure the consistent application of data protection law. They play a key role in safeguarding individuals' data protection rights, especially through exercising corrective powers. The EDPB website includes a selection of [SA supervisory actions](#) relating to GDPR enforcement at a national level. The EDPB also maintains a [register](#) of decisions taken by national SAs in line with the One-Stop-Shop cooperation procedure (Art. 60 GDPR).

#### 3.1. CROSS-BORDER COOPERATION

One of the SAs' tasks is to coordinate decision-making in cross-border data processing cases.

Between 1 January and 31 December 2021, there were 506 entries of cross-border cases in the database out of which 375 originated from a complaint, while 131 had other origins, such as investigations, legal obligations and/or media reports.

The One-Stop-Shop mechanism necessitates cooperation between the LSA and the CSAs. The LSA leads the investigation and plays a key role in the process of reaching a consensus between the CSAs, in addition to working towards reaching a coordinated decision about the data controller or processor. Between 1 January 2021 and 31 December 2021, there were 209 draft decisions, which resulted in 141 final decisions.

The mutual assistance procedure allows SAs to ask for information from other SAs or to request other measures for effective cooperation, such as prior authorisations or investigations. Between 1 January 2021 and 31 December 2021, SAs initiated 243 formal mutual assistance procedures and 2418 voluntary mutual assistance procedures.

#### **4. STAKEHOLDER CONSULTATION**

The EDPB conducted a survey as part of the annual review of the EDPB's activities under Art. 71(2) GDPR. Questions centred on the EDPB's work and output in 2021, with a focus on its guidelines and recommendations, all with a view to understanding the extent to which stakeholders find the EDPB's guidance helpful in interpreting the GDPR's provisions, and in order to identify future paths to better support individuals and organisations as they interact with the EU data protection framework.

#### **5. STRATEGY AND OBJECTIVES FOR 2022**

The EDPB's Strategy for 2021-2023 includes four main pillars, as well as a set of three key actions per pillar to help achieve these goals. In early 2021, the EDPB adopted its two-year work programme for 2021-2022, according to Art. 29 of the EDPB Rules of Procedure. The work programme follows the priorities set out in the Strategy and will put these into practice.

#### **CONTACT DETAILS**

Postal address  
Rue Wiertz 60, B-1047 Brussels

Office address  
Rue Montoyer 30, B-1000 Brussels

# Opinion of the Board (Art. 64)



**Opinion 11/2022 on the draft decision of the competent supervisory authority of Poland regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)**

**Adopted on 4 July 2022**

## Table of contents

1	Summary of the Facts .....	4
2	Assessment .....	4
2.1	General reasoning of the EDPB regarding the submitted draft decision .....	4
2.2	Main points of focus for the assessment (art. 43.2 GDPR and Annex 1 to the EDPB Guidelines) that the accreditation requirements provide for the following to be assessed consistently:.....	5
2.2.1	PREFIX .....	6
2.2.2	GENERAL REMARKS.....	6
2.2.3	GENERAL REQUIREMENTS FOR ACCREDITATION.....	7
2.2.4	RESOURCE REQUIREMENTS .....	7
2.2.5	PROCESS REQUIREMENTS.....	8
2.2.6	MANAGEMENT SYSTEM REQUIREMENTS.....	9
2.2.7	FURTHER ADDITIONAL REQUIREMENTS .....	9
3	Conclusions / Recommendations.....	9
4	Final Remarks .....	10

## The European Data Protection Board

Having regard to Article 63, Article 64 (1c), (3) - (8) and Article 43 (3) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,<sup>1</sup>

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

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (hereafter GDPR) throughout the European Economic Area. In compliance with Article 64.1 GDPR, the Board shall issue an opinion where a supervisory authority (SA) intends to approve the requirements for the accreditation of certification bodies pursuant to Article 43. The aim of this opinion is therefore to create a harmonised approach with regard to the requirements that a data protection supervisory authority or the National Accreditation Body will apply for the accreditation of a certification body. Even though the GDPR does not impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by encouraging SAs to draft their requirements for accreditation following the structure set out in the Annex to the EDPB Guidelines on accreditation of certification bodies, and, secondly by analysing them using a template provided by EDPB allowing the benchmarking of the requirements (guided by ISO 17065 and the EDPB guidelines on accreditation of certification bodies).

(2) With reference to Article 43 GDPR, the competent supervisory authorities shall adopt accreditation requirements. They shall, however, apply the consistency mechanism in order to allow generation of trust in the certification mechanism, in particular by setting a high level of requirements.

(3) While requirements for accreditation are subject to the consistency mechanism, this does not mean that the requirements should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB opinion is not to reach a single EU set of requirements but rather to avoid significant inconsistencies that may affect, for instance trust in the independence or expertise of accredited certification bodies.

(4) The "Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)" (hereinafter the "Guidelines"), and "Guidelines 1/2018 on certification and identifying certification criteria in accordance with article 42 and 43 of the Regulation 2016/679" will serve as a guiding thread in the context of the consistency mechanism.

(5) If a Member State stipulates that the certification bodies are to be accredited by the supervisory authority, the supervisory authority should establish accreditation requirements including, but not

---

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

limited to, the requirements detailed in Article 43(2). In comparison to the obligations relating to the accreditation of certification bodies by national accreditation bodies, Article 43 provides fewer details about the requirements for accreditation when the supervisory authority conducts the accreditation itself. In the interests of contributing to a harmonised approach to accreditation, the accreditation requirements used by the supervisory authority should be guided by ISO/IEC 17065 and should be complemented by the additional requirements a supervisory authority establishes pursuant to Article 43(1)(b). The EDPB notes that Article 43(2)(a)-(e) reflect and specify requirements of ISO 17065 which will contribute to consistency.<sup>2</sup>

(6) The opinion of the EDPB shall be adopted pursuant to Article 64 (1)(c), (3) & (8) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

## **HAS ADOPTED THE OPINION:**

### **1 SUMMARY OF THE FACTS**

1. The Polish SA (hereinafter “PL SA”) has submitted its draft accreditation requirements under Article 43 (1)(b) to the EDPB. The file was deemed complete on 28 March 2022. The national accreditation body (NAB) will perform accreditation of certification bodies to certify using GDPR certification criteria. This means that the NAB will use ISO 17065 and the additional requirements set up by the XX SA, once they are approved by the PL SA, following an opinion from the Board on the draft requirements, to accredit certification bodies. The PL SA will perform accreditation of certification bodies to certify using GDPR certification criteria.
2. In compliance with article 10 (2) of the Board Rules of Procedure, due to the complexity of the matter at hand, the Chair decided to extend the initial adoption period of eight weeks by a further six weeks.

### **2 ASSESSMENT**

#### **2.1 General reasoning of the EDPB regarding the submitted draft decision**

3. The purpose of this opinion is to assess the accreditation requirements developed by a SA, either in relation to ISO 17065 or a full set of requirements, for the purposes of allowing a national accreditation body or a SA, as per article 43(1) GDPR, to accredit a certification body responsible for issuing and renewing certification in accordance with article 42 GDPR. This is without prejudice to the tasks and powers of the competent SA. In this specific case, the Board notes that the PL SA has decided to resort to its national accreditation body (NAB) for the issuance of accreditation, having put together additional requirements in accordance with the Guidelines, which should be used by its NAB when

---

<sup>2</sup> Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation, par. 39. Available at: [https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies\\_en](https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_en)

issuing accreditation. In this specific case, the Board notes that the PL SA is tasked by national law to carry out the accreditation of certification bodies. To this end, the PL SA has developed a set of requirements specifically for accreditation of certification bodies in conjunction with a set of certification criteria that is yet to be formally approved.

4. This assessment of PL SA's additional accreditation requirements is aimed at examining on variations (additions or deletions) from the Guidelines and notably their Annex 1. Furthermore, the EDPB's Opinion is also focused on all aspects that may impact on a consistent approach regarding the accreditation of certification bodies.
5. It should be noted that the aim of the Guidelines on accreditation of certification bodies is to assist the SAs while defining their accreditation requirements. The Guidelines' Annex does not constitute accreditation requirements as such. Therefore, the accreditation requirements for certification bodies need to be defined by the SA in a way that enables their practical and consistent application as required by the SA's context.
6. The Board acknowledges the fact that, given their expertise, freedom of manoeuvre should be given to NABs when defining certain specific provisions within the applicable accreditation requirements. However, the Board considers it necessary to stress that, where any additional requirements are established, they should be defined in a way that enables their practical, consistent application and review as required.
7. The Board notes that ISO standards, in particular ISO 17065, are subject to intellectual property rights, and therefore it will not make reference to the text of the related document in this Opinion. As a result, the Board decided to, where relevant, point towards specific sections of the ISO Standard, without, however, reproducing the text.
8. Finally, the Board has conducted its assessment in line with the structure foreseen in Annex 1 to the Guidelines (hereinafter "Annex"). Where this Opinion remains silent on a specific section of the PL SA's draft accreditation requirements, it should be read as the Board not having any comments and not asking the PL SA to take further action.
9. This opinion does not reflect upon items submitted by the PL SA, which are outside the scope of article 43 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

## **2.2 Main points of focus for the assessment (art. 43.2 GDPR and Annex 1 to the EDPB Guidelines) that the accreditation requirements provide for the following to be assessed consistently:**

- a. addressing all the key areas as highlighted in the Guidelines Annex and considering any deviation from the Annex.
- b. independence of the certification body
- c. conflicts of interests of the certification body
- d. expertise of the certification body
- e. appropriate safeguards to ensure GDPR certification criteria is appropriately applied by the certification body

- f. procedures for issuing, periodic review and withdrawal of GDPR certification; and
  - g. transparent handling of complaints about infringements of the certification.
10. Taking into account that:
- a. Article 43 (2) GDPR provides a list of accreditation areas that a certification body need to address in order to be accredited;
  - b. Article 43 (3) GDPR provides that the requirements for accreditation of certification bodies shall be approved by the competent Supervisory Authority;
  - c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for certification bodies and may decide to conduct the accreditation of certification bodies itself;
  - d. Article 64 (1) (c) GDPR provides that the Board shall issue an opinion where a supervisory authority intends to approve the accreditation requirements for a certification body pursuant to Article 43(3);
  - e. If accreditation is carried out by the national accreditation body in accordance with ISO/IEC 17065/2012, the additional requirements established by the competent supervisory authority must also be applied;
  - f. Annex 1 of the Guidelines on Accreditation of Certification foresees suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a certification body by the National Accreditation Body;

the Board is of the opinion that:

### 2.2.1 PREFIX

11. The Board acknowledges the fact that terms of cooperation regulating the relationship between a National Accreditation Body and its data protection supervisory authority are not a requirement for the accreditation of certification bodies *per se*. However, for reasons of completeness and transparency, the Board considers that such terms of cooperation, where existing, shall be made public in a format considered appropriate by the SA.

### 2.2.2 GENERAL REMARKS

12. The Board notes that some terms, for instance section 7.4 of the draft requirements refer to “targets of assessment” instead of “targets of evaluation” and to the term “assessment” instead of “certification”. The Board considers that these terms are not in accordance with the Guidelines. Therefore, the Board encourages the PL SA to modify such terms so to bring them in line with the Guidelines.
13. The Board welcomes the reference “The wide range of ISO/IEC 17065/2012, covering products, processes and services, should not lead to lowering or substitution of GDPR requirements” in section 1 of the draft requirements. However the Board is of the Opinion that the precedence of the GDPR over the ISO/IEC 17065/2012 should be made explicitly in the requirements, pursuant to Annex 1

14. The Board notes that in section 1 of the PL SA's draft accreditation requirements, the PL SA makes a distinction between controller, processor and manufacturers or the entity marketing a service product. The Board's understanding is that both manufacturers and the entity marketing a service or product are either controllers or processors, thus the Board is not concerned by this distinction.

### 2.2.3 GENERAL REQUIREMENTS FOR ACCREDITATION

15. With respect to section 4.1.2 of the PL SA's draft accreditation requirements, the Board notes that in paragraph 5 of this section, the requirement of the Guidelines "the certification program and other regulations must be observed and adhered to" is missing. Therefore, the Board recommends the PL SA to complete this requirement accordingly.
16. Regarding section 4.1.2 of the PL SA's draft accreditation requirements, the Board notes there is a reference to certification body's obligation to "indicate" the consequences to the Customer in paragraph 9. With respect to this requirement, section 4.1.2 para. 9 of the Annex establishes that the consequences for the customer in those cases shall be addressed. The Board understands that the intention of the PL SA is to ensure that the client is aware of the consequences in those situations and of the potential options or actions that can be taken. However, the Board considers that, in order to ensure that certification agreements accurately reflect not only the consequences and impact on the clients, but also the potential further actions, the PL SA's accreditation requirements should make clear that simply stating the consequences without addressing the potential next steps won't be sufficient. Thus, the Board encourages the PL SA to make clear that the customer should be aware of the consequences, the impact they have on them and the potential next steps that may be taken.
17. With regard to the section 4.3 of the draft requirements, the Board welcomes the inclusion the reference on liability and finances "In addition to the requirement set out in point 4.3.1 of ISO/IEC 17065/2012, the PCA shall ensure on a regular basis that the Certification Body has appropriate measures (e.g. insurance or reserves) to cover its liabilities." However the Board wish to highlight that the PL SA omitted to include that the cover of liabilities refers to the geographical regions in which the NAB operates. Therefore, the Board recommends the PL SA to add this element to this requirement so to align it with the Guidelines.
18. Regarding section 4.6 of the PL SA's draft accreditation requirements, the certification body is required to provide "1) all versions (current and previous) of the approved criteria used within the meaning of Article 42(5) of the GDPR (certification criteria) are published and easily publicly available, as well as all certification procedures, generally stating a relevant period of validity and 2) information on complaint and appeal procedures are made public in accordance with Article 43(2)(d) of the GDPR." The Board encourages the PL SA to add in the requirements that this is information shall be provided at minimum, according to section 4.6 ISO/IEC 17065/2012.

### 2.2.4 RESOURCE REQUIREMENTS

19. As a general remark, the Board considers that the expertise requirements for evaluators and decision-makers should be tailored taking into account the different tasks that they perform. In this regard, the Board is of the opinion that evaluators should have a more specialist expertise and professional experience in technical procedures (e.g. audits and certifications), whereas decision-makers should have a more general and comprehensive expertise and professional experience in data protection. Considering this, the Board encourages the PL SA to redraft this subsection taking into account the

different substantive knowledge and/or experience requirements for evaluators and decision-makers, rather than the years of experience.

20. In section 6.1 of the PL SA's draft accreditation requirements, it is mentioned that "the certification body is responsible for making decisions even if it is assisted by sub-contractors". Right below it is mentioned that the "subcontractors should not be involved in decision-making processes". The Board recommends the PL SA to modify this requirement so to clarify that when the certification body uses subcontractors the certification body is the one responsible for the decision-making.

## 2.2.5 PROCESS REQUIREMENTS

21. With regard to section 7.1(2) of the draft requirements, the Board underlines that, even when an EU Data Protection Seal has been approved, the certification body still has to notify the relevant CSAs before operating it in a new Member State from a satellite office. This is especially relevant, considering that accreditation of a certification body granting European Data Protection Seals may have to be carried out in each of the Members States where the certification body is established.<sup>3</sup> However, it shall be noted that the CSAs should be notified even in those cases in which the operation of an EU Data Protection Seal in a new Member State does not require a new accreditation. Therefore, the Board recommends the PL SA to include the above-mentioned reference. For example, the draft requirements could state the following (see proposed amendments in italics): "If the certification body intends to act in other Member States, it shall notify and, when necessary, obtain the necessary approval from the relevant competent authorities, including for the operation of a European Data Protection Seal in accordance with Article 42(5) of the GDPR".
22. Similarly, in the same section, the Board encourages the PL SA to bring the draft accreditation requirements in line with the Guidelines, by adding "from a satellite office", that is currently missing from the draft.
23. Concerning paragraph 4 of section 7.1(4) and 7.2(4) of the draft requirements of the PL SA's, the Board notes that It should be clear that such investigation should be linked with the scope of certification and the target of evaluation. Therefore, the Board recommends that the PL SA amend its requirement accordingly, by specifying that the investigation should be linked to the scope of certification and the target of evaluation.
24. In section 7.4(1) the Board encourages the PL SA to add the missing term "concerned" before the data subjects so to bring this requirement in line with the Guidelines.
25. In section 7.4(2) the Board encourages the PL SA to replace the term "applicants" with "controller and processor".
26. In section 7.4(2) the Board notes that this reference "*However, the certificate itself will not be a sufficient proof and the Certification Body shall be obliged to verify compliance with the criteria in relation to the object of the assessment*" misses an element provided in the criteria (i.e. that this is not sufficient to completely replace partial evaluations). The Board recommends the PL SA to add this element to the draft requirements so to bring them in line with the Guidelines.
27. In the same section, the last part of the paragraph from the Guidelines is missing "...*a certification statement or similar certification certificates should not be considered sufficient to replace a report*". The Board recommends the PL SA to complete the requirement accordingly.

- 28. In section 7.8 “directory of certified products” the Board recommends the PL SA to modify the draft requirements and clearly state that the certification body shall inform not only the Supervisory authority of the reasons for granting or revoking or refusing the requested certification, but also any other competent supervisory authorities.
- 29. The Board welcomes, in section 7.10 of the draft accreditation requirements, the inclusion of personal data breaches and infringements of the GDPR in the list of changes that can affect certification. However, in order to ensure clarity, the Board encourages the PL SA to specify that the data breaches or infringements of the GDPR shall be taken into account only inasmuch as they relate to the certification.
- 30. With regards to the section 7.11 of the draft accreditation requirements on “termination, reduction, suspension or withdrawal of certification”, regarding the obligation of the certification body to inform the supervisory authority of the measures taken about the continuation, restriction, suspension and revocation of certification, it is not specified that this should be in writing. The Board thus encourages the PL SA to clarify this requirement by adding that this information obligation will take place in writing.

## 2.2.6 MANAGEMENT SYSTEM REQUIREMENTS

- 31. With regard to section 8 of the draft accreditation requirements on “management systems requirements” of the draft accreditation requirements, the Board notes that the below two paragraphs of the Guidelines (section 8) are missing:
    - 1. These management principles and their documented implementation must be transparent and be disclosed by the accredited certification body pursuant in the accreditation procedure pursuant to Article 58 and thereafter at the request of the data protection supervisory authority at any time during an investigation in the form of data protection reviews pursuant to Art. 58(1)(b) or a review of the certifications issued in accordance with Article 42(7) pursuant to Article 58(1)(c).
    - 2. In particular, the accredited certification body must make public permanently and continuously which certifications were carried out on which basis (or certification mechanisms or schemes), how long the certifications are valid under which framework and conditions (recital 100).
- Thus the Board recommends the PL SA to add these two paragraphs so to complete the draft requirements.

## 2.2.7 FURTHER ADDITIONAL REQUIREMENTS

- 32. With respect to 9.3.1 of the draft accreditation requirements, the Board encourages to clarify that it is the responsibility of the certification body and add not only customers but also applicants.

# 3 CONCLUSIONS / RECOMMENDATIONS

- 33. The draft accreditation requirements of the PL Supervisory Authority may lead to an inconsistent application of the accreditation of certification bodies and the following changes need to be made:
- 34. Regarding ‘general remarks’, the Board recommends that the PL SA:

- 1) completes the requirement of section 4.1.2 (paragraph 5) by adding that the “certification program and other regulations must be observed and adhered to it”.
  - 2) adds to section 4.3 of the requirements that the cover of liabilities refers also to geographical regions that the NAB operates.
35. Regarding ‘resource requirements’, the Board recommends that the PL SA:
  - 1) modifies the requirement of section 6.1 so to clarify that when the certification body uses sub-contractors the certification body is the one responsible for the decision-making.
36. Regarding ‘process requirements’, the Board recommends that the PL SA:
  - 1) includes a reference in section 7.1(2) to the fact that even when an EU Data Protection Seal is approved, the certification body still has to notify the relevant CSAs before operating in a new Member state from a satellite office.
  - 2) amends the requirement of section 7.1(3) and 7.2(4) by specifying that the investigation should be linked to scope of certification and target of evaluation.
  - 3) includes in section 7.4(2), in addition to the reference “However, the certificate itself will not be a sufficient proof and the Certification Body shall be obliged to verify compliance with the criteria in relation to the object of the assessment”, that this is not sufficient to completely replace partial evaluations.
  - 4) completes the last paragraph of the same section, by adding that “...a certification statement or similar certification certificates should not be considered sufficient to replace a report”.
  - 5) modifies the draft requirements in section 7.8 and clearly state that the certification body shall inform not only the Supervisory authority of the reasons for granting or revoking or refusing the requested certification, but also any other competent authorities.
37. Regarding ‘management system requirements’, the Board recommends that the PL SA:
  - 1) adds, in section 8 of the draft requirement, the two paragraphs, that comparing to the Guidelines, section 8 are missing.

## 4 FINAL REMARKS

38. This opinion is addressed to the Polish Supervisory Authority and will be made public pursuant to Article 64 (5)(b) GDPR.
39. According to Article 64 (7) and (8) GDPR, the PL SA shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.
40. The PL SA shall communicate the final decision to the Board for inclusion in the register of decisions, which have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

# Opinion of the Board (Art. 64)



**Opinion 12/2022 on the draft decision of the competent supervisory authority of France regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)**

**Adopted on 4 July 2022**

## Table of contents

1	Summary of the Facts .....	4
2	Assessment .....	4
2.1	General reasoning of the EDPB regarding the submitted draft decision .....	4
2.2	Main points of focus for the assessment (art. 43.2 GDPR and Annex 1 to the EDPB Guidelines) that the accreditation requirements provide for the following to be assessed consistently:.....	5
2.2.1	PREFIX .....	6
2.2.2	GENERAL REMARKS.....	6
2.2.3	GENERAL REQUIREMENTS FOR ACCREDITATION.....	6
2.2.4	RESOURCE REQUIREMENTS .....	7
2.2.5	PROCESS REQUIREMENTS.....	8
2.2.6	MANAGEMENT SYSTEM REQUIREMENTS.....	9
3	Conclusions / Recommendations.....	9
4	Final Remarks .....	10

## The European Data Protection Board

Having regard to Article 63, Article 64 (1c), (3) - (8) and Article 43 (3) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,<sup>1</sup>

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

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (hereafter GDPR) throughout the European Economic Area. In compliance with Article 64.1 GDPR, the Board shall issue an opinion where a supervisory authority (SA) intends to approve the requirements for the accreditation of certification bodies pursuant to Article 43. The aim of this opinion is therefore to create a harmonised approach with regard to the requirements that a data protection supervisory authority or the National Accreditation Body will apply for the accreditation of a certification body. Even though the GDPR does not impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by encouraging SAs to draft their requirements for accreditation following the structure set out in the Annex to the EDPB Guidelines on accreditation of certification bodies, and, secondly by analysing them using a template provided by EDPB allowing the benchmarking of the requirements (guided by ISO 17065 and the EDPB guidelines on accreditation of certification bodies).

(2) With reference to Article 43 GDPR, the competent supervisory authorities shall adopt accreditation requirements. They shall, however, apply the consistency mechanism in order to allow generation of trust in the certification mechanism, in particular by setting a high level of requirements.

(3) While requirements for accreditation are subject to the consistency mechanism, this does not mean that the requirements should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB opinion is not to reach a single EU set of requirements but rather to avoid significant inconsistencies that may affect, for instance trust in the independence or expertise of accredited certification bodies.

(4) The "Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)" (hereinafter the "Guidelines"), and "Guidelines 1/2018 on certification and identifying certification criteria in accordance with article 42 and 43 of the Regulation 2016/679" will serve as a guiding thread in the context of the consistency mechanism.

(5) If a Member State stipulates that the certification bodies are to be accredited by the supervisory authority, the supervisory authority should establish accreditation requirements including, but not

---

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

limited to, the requirements detailed in Article 43(2). In comparison to the obligations relating to the accreditation of certification bodies by national accreditation bodies, Article 43 provides fewer details about the requirements for accreditation when the supervisory authority conducts the accreditation itself. In the interests of contributing to a harmonised approach to accreditation, the accreditation requirements used by the supervisory authority should be guided by ISO/IEC 17065 and should be complemented by the additional requirements a supervisory authority establishes pursuant to Article 43(1)(b). The EDPB notes that Article 43(2)(a)-(e) reflect and specify requirements of ISO 17065 which will contribute to consistency.<sup>2</sup>

(6) The opinion of the EDPB shall be adopted pursuant to Article 64 (1)(c), (3) & (8) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

## **HAS ADOPTED THE OPINION:**

### **1 SUMMARY OF THE FACTS**

1. The French Supervisory Authority (hereinafter “FR SA”) has submitted its draft accreditation requirements under Article 43 (1)(b) to the EDPB. The file was deemed complete on 29 March 2022. The FR national accreditation body (NAB) will perform accreditation of certification bodies to certify using GDPR certification criteria. This means that the NAB will use ISO 17065 and the additional requirements set up by the FR SA, once they are approved by the FR SA, following an opinion from the Board on the draft requirements, to accredit certification bodies.

### **2 ASSESSMENT**

#### **2.1 General reasoning of the EDPB regarding the submitted draft decision**

2. The purpose of this opinion is to assess the accreditation requirements developed by a SA, either in relation to ISO 17065 or a full set of requirements, for the purposes of allowing a national accreditation body or a SA, as per article 43(1) GDPR, to accredit a certification body responsible for issuing and renewing certification in accordance with article 42 GDPR. This is without prejudice to the tasks and powers of the competent SA. In this specific case, the Board notes that the FR SA has decided to resort to its national accreditation body (NAB) for the issuance of accreditation, having put together additional requirements in accordance with the Guidelines, which should be used by its NAB when issuing accreditation.
3. This assessment of FR SA’s additional accreditation requirements is aimed at examining on variations (additions or deletions) from the Guidelines and notably their Annex 1. Furthermore, the EDPB’s

---

<sup>2</sup> Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation, par. 39. Available at: [https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies\\_en](https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_en)

Opinion is also focused on all aspects that may impact on a consistent approach regarding the accreditation of certification bodies.

4. It should be noted that the aim of the Guidelines on accreditation of certification bodies is to assist the SAs while defining their accreditation requirements. The Guidelines' Annex does not constitute accreditation requirements as such. Therefore, the accreditation requirements for certification bodies need to be defined by the SA in a way that enables their practical and consistent application as required by the SA's context.
5. The Board acknowledges the fact that, given their expertise, freedom of manoeuvre should be given to NABs when defining certain specific provisions within the applicable accreditation requirements. However, the Board considers it necessary to stress that, where any additional requirements are established, they should be defined in a way that enables their practical, consistent application and review as required.
6. The Board notes that ISO standards, in particular ISO 17065, are subject to intellectual property rights, and therefore it will not make reference to the text of the related document in this Opinion. As a result, the Board decided to, where relevant, point towards specific sections of the ISO Standard, without, however, reproducing the text.
7. Finally, the Board has conducted its assessment in line with the structure foreseen in Annex 1 to the Guidelines (hereinafter "Annex"). Where this Opinion remains silent on a specific section of the FR SA's draft accreditation requirements, it should be read as the Board not having any comments and not asking the FR SA to take further action.
8. This opinion does not reflect upon items submitted by the FR SA, which are outside the scope of article 43 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

## **2.2 Main points of focus for the assessment (art. 43.2 GDPR and Annex 1 to the EDPB Guidelines) that the accreditation requirements provide for the following to be assessed consistently:**

- a. addressing all the key areas as highlighted in the Guidelines Annex and considering any deviation from the Annex.
  - b. independence of the certification body
  - c. conflicts of interests of the certification body
  - d. expertise of the certification body
  - e. appropriate safeguards to ensure GDPR certification criteria is appropriately applied by the certification body
  - f. procedures for issuing, periodic review and withdrawal of GDPR certification; and
  - g. transparent handling of complaints about infringements of the certification.
9. Taking into account that:

- a. Article 43 (2) GDPR provides a list of accreditation areas that a certification body need to address in order to be accredited;
- b. Article 43 (3) GDPR provides that the requirements for accreditation of certification bodies shall be approved by the competent Supervisory Authority;
- c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for certification bodies and may decide to conduct the accreditation of certification bodies itself;
- d. Article 64 (1) (c) GDPR provides that the Board shall issue an opinion where a supervisory authority intends to approve the accreditation requirements for a certification body pursuant to Article 43(3);
- e. If accreditation is carried out by the national accreditation body in accordance with ISO/IEC 17065/2012, the additional requirements established by the competent supervisory authority must also be applied;
- f. Annex 1 of the Guidelines on Accreditation of Certification foresees suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a certification body by the National Accreditation Body;

the Board is of the opinion that:

#### [2.2.1 PREFIX](#)

10. The Board acknowledges the fact that terms of cooperation regulating the relationship between a National Accreditation Body and its data protection supervisory authority are not a requirement for the accreditation of certification bodies *per se*. However, for reasons of completeness and transparency, the Board considers that such terms of cooperation, where existing, shall be made public in a format considered appropriate by the SA.

#### [2.2.2 GENERAL REMARKS](#)

11. Section 5 of the draft accreditation requirements mentions that the CB shall inform the NAB regarding any other binding decision that may constitute a non-conformity to the requirements of this document. The EDPB encourages the FR SA to redraft this requirement so to include explicitly the decisions of the competent judicial authorities that may affect the accreditation.
12. In general, the Board encourages the FR SA to ensure consistency of the wording throughout the text (e.g. translation problem in section 4.6 heading). Similarly in section 7(3)(3)(f), there is a new term introduced, this of “candidate” instead of applicant.

#### [2.2.3 GENERAL REQUIREMENTS FOR ACCREDITATION](#)

13. Regarding section 4.1 “legal responsibility”, the Board encourages the FR SA to explicitly refer to up-to-date procedures and measures.
14. With respect to section 4.1.2(2) letter b, states that “the methods to be applied by the certification body for the assessment of the target of evaluation, as defined in the requirements in §7.3(2) b) of

this document”. In this regard, the Board, for the sake of clarity, encourages the FR SA to redraft this requirement and bring it in line with the Guidelines (section 7(3)(1) of the Annex), by explicitly referring to binding character of the evaluation methods.

15. Concerning section 4.1.2(2) letter c of FR SA’s draft accreditation requirements, regarding the organisation and the procedures to be put in place by the certification body for complaint and appeal management, the Board encourages the FR SA to bring it line with the Guidelines (section 4.1(8)) by adding the reference to “additionally, lit. j, shall also contain explicit statements on the structure and the procedure for complaint management in accordance with Article. 43(2)(d);”.
16. Regarding section 4.1.3(1), letter a of the draft accreditation requirements, the FR SA refers to “certification mechanism is clearly referenced, and, where applicable, the subset of the criteria applicable to the target of evaluation is indicated”. The Board encourages the FR SA to further explain in the requirements the essence of this concept of the subset of the criteria.
17. Regarding section 4.2 “management of impartiality”, the Board notes that the draft accreditation requirements make reference only to rules to prevent the conflict of interest. The Board acknowledges the importance to have requirements to ensure, firstly, that there are no conflicts of interest and, secondly in case conflicts of interest are identified, that the certification body manages them. Therefore, the Board encourages the FR SA, in addition to having rules preventing conflicts, there should be clear rules to manage identified conflicts of interest.
18. Regarding section 4.2(b) “it is not affiliated to the client’s organization nor does it share the same holding than its client”, the Board encourages the FR SA to clarify the wording, in order to reflect the independence of the certification body. For example, the FR SA could state that the certification body should not belong to the same company group nor should be controlled in any way by the customer it assesses.
19. According to the Guidelines (Annex, section 4.1.2.2 “ the certification body shall demonstrate in addition to requirements of ISO/IEC 17065/2012 that its certification agreements: require the applicant to allow full transparency to the competent supervisory authority with respect to the certification procedure, including **contractually confidential matters** related to data protection compliance”. The Board notes that the explicit reference to the “contractually confidential matters” is missing in section 4.5 “confidentiality” of the draft accreditation requirements, thus the Board recommends the FR SA to include explicitly the obligation of the certification body to provide access to the SA to **contractually confidential matters**.
20. With respect to section 4.5.b of the FR SA’s draft accreditation requirements, the Board encourages the FR SA to slightly modify the wording “the information to be published by the CNIL in the registry of certifications” and add submitted to the CNIL instead.

#### 2.2.4 RESOURCE REQUIREMENTS

21. Regarding section 6.1(1) letters b and c, the Board recommends the FR SA to bring these in line with the Guidelines and add appropriate and relevant knowledge instead of appropriate experience.
22. With respect to section 6.1(3) last paragraph of the draft accreditation requirements, the latter make a reference to the scenario “when the personnel responsible for certification decisions does not have such knowledge and experience in personal data protection [...]. The Board understands that this refers to solely one decision that needs to be taken and for which the personnel lacks experience and

knowledge, but this does not in any way refer to the decision-making of the certification body as a whole. To avoid any confusion, the Board recommends that the FR SA further explains this in the requirements.

23. Similarly, in section 6.1(4) the Board recommends the FR SA to clarify what “Such expertise is not necessarily concentrated by one single individual. For instance it can be shared among the members of an evaluation team”.
24. Section 6.2 “resources for evaluation” the Board recommends the FR SA to clarify that the certification body will retain the responsibility for the decision-making even when it uses external experts/bodies.

## 2.2.5 PROCESS REQUIREMENTS

25. With regards to section 7.2(1) letter h, the Board encourages the FR SA to clarify which information on recent sanction decisions and/or corrective measures imposed by the CNIL or other supervisory authorities to the applicant shall be obtained by the certification body. More precisely, the notion of “recent” needs elaboration. The same also applies for the Section 7.3(2) letter b.
26. With respect to section 7.2(1) letter h, the Board notes the reference to “information related to ongoing investigations, or recent sanction decisions and/or corrective measures imposed by CNIL or other supervisory authorities”. However, for clarity purposes, the Board encourages the FR SA to clearly state that these are authorities, refer to competent authorities.
27. Regarding Section 7.4(2) letter b of the draft accreditation requirements “a method for evaluating the coverage, the type and assessment of all risks considered by the controller and the processor with regard to their obligations pursuant to Articles 30, 32 and 35 and 36 of the GDPR, and with regard to the appropriateness of technical and organisational measures pursuant to Articles 24, 25 and 32 of the GDPR”, the Board encourages the FR SA to bring this requirement in line with the Guidelines, by adding “insofar as the aforementioned Articles apply to the object of certification”.
28. With respect to section 7.4(3) of the FR SA’s draft accreditation requirements, where it is mentioned that “where the certification body assigns to the evaluation tasks personnel that does not meet the “technical profile” nor the “legal profile” requirements (as defined in para. 6 of the requirements), it shall justify the need for assigning an “expert” with specific competencies for the need of the evaluation”. The Board understands that this will in case in exceptional circumstances, where there will be a need for specific expertise, which the certification body’s personnel will not have. However, the Board encourages the FR SA to appropriately rephrase this requirement so to avoid confusion.
29. As regards to section 7(5)(1) of the FR SA’s draft accreditation requirements, the Board encourages the FR SA to clarify that the review of the process, as mentioned in section 7.5 of the Annex of the Guidelines, is to be conducted in line with section 7.9(2) of the draft certification requirements, where the regularity of the surveillance activities is required .
30. Regarding Section 7.8(1)(b) of the FR SA’s accreditation requirements, the Board recommends that the FR SA amends this requirement so to ensure that, in line with the Guidelines, a meaningful description on the object of certification is in place.
31. With respect to the same section (note 1), where FR SA mentions that “this information does not have to be made public, contrary to the information detailed in section 7.8(2) of this document but shall be made available upon request to third parties that wish to make sure of the validity of a certification”, the Board encourages the FR SA to clarify in the requirements why this distinction is made therein.

32. Regarding section 7.9(2) last paragraph of the FR SA's draft accreditation requirements, the Board encourages the FR SA to clarify that it will provide this information to CNIL in writing.
33. Concerning Section 7.10(2), the Board acknowledges that according to the FR SA's draft accreditation requirements, where there are changes affecting the certification process, the evaluation of the criteria shall be conducted, where required (see letter c in this section). However, the formulation in letter b may lead to misconceptions that such an immediate complementary evaluation or re-evaluation of the certification criteria will not be the case. Therefore, the Board encourages the FR SA to re-formulate this point to avoid any ambiguity by adding a first indent, requiring the documentation of an immediate complementary evaluation or re-evaluation of the certification criteria

## 2.2.6 MANAGEMENT SYSTEM REQUIREMENTS

34. Regarding section 8.1(1) of the FR SA's draft accreditation requirements, the Board recommends that the FR SA brings this section in line with the Guidelines, Annex, section 8, by ensuring to add the following to the requirements that the management system must specify a methodology for achieving and controlling these requirements in compliance with data protection regulations and for continuously checking them with the accredited body itself.
35. Regarding section to 8.1(2) the Board notes that to provide information must be disclosed at **any time**, and not only during the accreditation procedure, is missing. In particular, the accredited certification body must make public permanently and continuously which certifications were carried out on which basis (or certification mechanisms or schemes), how long the certifications are valid under which framework and conditions (recital 100). Therefore the Board recommends that the FR SA adds this to the accreditation requirements so to bring them in line with the Annex, section 8, of the Guidelines.

## 3 CONCLUSIONS / RECOMMENDATIONS

36. The draft accreditation requirements of the FR Supervisory Authority may lead to an inconsistent application of the accreditation of certification bodies and the following changes need to be made:
37. Regarding 'general requirements for accreditation', the Board recommends that the FR SA:
  - 1) includes in section 4.5 of the draft requirements an explicit reference to the obligation of the certification body to provide access to the SA to contractually confidential matters.
38. Regarding 'resource requirements', the Board recommends that the FR SA:
  - 1) redrafts the requirement of section 6.1.(1) letters b and c so to refer to appropriate and relevant knowledge instead of appropriate expertise.
  - 2) further explains in the section 6.1(3) last paragraph, that "when the personnel responsible for certification decisions does not have such knowledge and experience in personal data protection [...]", this refers to solely one decision that needs to be taken and for which the personnel lacks experience and knowledge, but this does not in any way refer to the decision-making of the certification body as a whole.

- 3) similarly, clarifies the reference to “such expertise is not necessarily concentrated by one single individual” in section 6.1(4) of the draft requirements.
  - 4) clarifies in section 6.2 of the draft requirements that the certification body will retain the responsibility for the decision-making even when it uses externals/bodies.
39. Regarding ‘process requirements’, the Board recommends that the FR SA:
- 1) amends section 7.8(1)(b) of the draft requirements, to ensure, that in line with the Guidelines, a meaningful description on the object of certification is in place.
40. Regarding ‘management system requirements’, the Board recommends that the FR SA:
- 1) adds the following to the requirements that the management system must specify a methodology for achieving and controlling these requirements in compliance with data protection regulations and for continuously checking them with the accredited body itself.
  - 2) includes that the information must be provided at any time.

## 4 FINAL REMARKS

41. This opinion is addressed to the French Supervisory Authority and will be made public pursuant to Article 64 (5)(b) GDPR.
42. According to Article 64 (7) and (8) GDPR, the FR SA shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.
43. The FR SA shall communicate the final decision to the Board for inclusion in the register of decisions, which have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

# Opinion of the Board (Art. 64)



**Opinion 13/2022 on the draft decision of the competent supervisory authority of Bulgaria regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)**

**Adopted on 4 July 2022**

## Table of contents

1	Summary of the Facts.....	4
2	Assessment.....	4
2.1	General reasoning of the EDPB regarding the submitted draft decision.....	4
2.2	Main points of focus for the assessment (art. 43.2 GDPR and Annex 1 to the EDPB Guidelines) that the accreditation requirements provide for the following to be assessed consistently: .....	5
2.2.1	GENERAL REMARKS.....	6
2.2.2	GENERAL REQUIREMENTS FOR ACCREDITATION .....	7
2.2.3	RESOURCE REQUIREMENTS .....	8
2.2.4	PROCESS REQUIREMENTS.....	9
2.2.5	MANAGEMENT SYSTEM REQUIREMENTS.....	10
2.2.6	FURTHER ADDITIONAL REQUIREMENTS .....	11
3	Conclusions / Recommendations.....	11
4	Final Remarks .....	13

## The European Data Protection Board

Having regard to Article 63, Article 64 (1c), (3) - (8) and Article 43 (3) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,<sup>1</sup>

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

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (hereafter GDPR) throughout the European Economic Area. In compliance with Article 64.1 GDPR, the Board shall issue an opinion where a supervisory authority (SA) intends to approve the requirements for the accreditation of certification bodies pursuant to Article 43. The aim of this opinion is therefore to create a harmonised approach with regard to the requirements that a data protection supervisory authority or the National Accreditation Body will apply for the accreditation of a certification body. Even though the GDPR does not impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by encouraging SAs to draft their requirements for accreditation following the structure set out in the Annex to the EDPB Guidelines on accreditation of certification bodies, and, secondly by analysing them using a template provided by EDPB allowing the benchmarking of the requirements (guided by ISO 17065 and the EDPB guidelines on accreditation of certification bodies).

(2) With reference to Article 43 GDPR, the competent supervisory authorities shall adopt accreditation requirements. They shall, however, apply the consistency mechanism in order to allow generation of trust in the certification mechanism, in particular by setting a high level of requirements.

(3) While requirements for accreditation are subject to the consistency mechanism, this does not mean that the requirements should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB opinion is not to reach a single EU set of requirements but rather to avoid significant inconsistencies that may affect, for instance trust in the independence or expertise of accredited certification bodies.

(4) The "Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)" (hereinafter the "Guidelines"), and "Guidelines 1/2018 on certification and identifying certification criteria in accordance with article 42 and 43 of the Regulation 2016/679" will serve as a guiding thread in the context of the consistency mechanism.

(5) If a Member State stipulates that the certification bodies are to be accredited by the supervisory authority, the supervisory authority should establish accreditation requirements including, but not limited to, the requirements detailed in Article 43(2). In comparison to the obligations relating to the

---

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

accreditation of certification bodies by national accreditation bodies, Article 43 provides fewer details about the requirements for accreditation when the supervisory authority conducts the accreditation itself. In the interests of contributing to a harmonised approach to accreditation, the accreditation requirements used by the supervisory authority should be guided by ISO/IEC 17065 and should be complemented by the additional requirements a supervisory authority establishes pursuant to Article 43(1)(b). The EDPB notes that Article 43(2)(a)-(e) reflect and specify requirements of ISO 17065 which will contribute to consistency.<sup>2</sup>

(6) The opinion of the EDPB shall be adopted pursuant to Article 64 (1)(c), (3) & (8) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

#### **HAS ADOPTED THE OPINION:**

## **1 SUMMARY OF THE FACTS**

1. The Bulgarian Supervisory Authority (hereinafter “BG SA”) has submitted its draft accreditation requirements under Article 43 (1)(b) to the EDPB. The file was deemed complete on 28 March 2022. The BG SA will perform accreditation of certification bodies to certify using GDPR certification criteria.
2. In compliance with article 10 (2) of the Board Rules of Procedure, due to the complexity of the matter at hand, the Chair decided to extend the initial adoption period of eight weeks by a further six weeks.

## **2 ASSESSMENT**

### **2.1 General reasoning of the EDPB regarding the submitted draft decision**

3. The purpose of this opinion is to assess the accreditation requirements developed by a SA, either in relation to ISO 17065 or a full set of requirements, for the purposes of allowing a national accreditation body or a SA, as per article 43(1) GDPR, to accredit a certification body responsible for issuing and renewing certification in accordance with article 42 GDPR. This is without prejudice to the tasks and powers of the competent SA. In this specific case, the Board notes that the BG SA is tasked by national law to carry out the accreditation of certification bodies. To this end, the BG SA has developed a set of requirements specifically for accreditation of certification bodies in conjunction with a set of certification criteria that is yet to be formally approved.
4. This assessment of BG SA’s additional accreditation requirements is aimed at examining on variations (additions or deletions) from the Guidelines and notably their Annex 1. Furthermore, the EDPB’s

---

<sup>2</sup> Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation, par. 39. Available at: [https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies\\_en](https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_en)

Opinion is also focused on all aspects that may impact on a consistent approach regarding the accreditation of certification bodies.

5. It should be noted that the aim of the Guidelines on accreditation of certification bodies is to assist the SAs while defining their accreditation requirements. The Guidelines' Annex does not constitute accreditation requirements as such. Therefore, the accreditation requirements for certification bodies need to be defined by the SA in a way that enables their practical and consistent application as required by the SA's context.
6. The Board acknowledges the fact that, given their expertise, freedom of manoeuvre should be given to NABs when defining certain specific provisions within the applicable accreditation requirements. However, the Board considers it necessary to stress that, where any additional requirements are established, they should be defined in a way that enables their practical, consistent application and review as required.
7. The Board notes that ISO standards, in particular ISO 17065, are subject to intellectual property rights, and therefore it will not make reference to the text of the related document in this Opinion. As a result, the Board decided to, where relevant, point towards specific sections of the ISO Standard, without, however, reproducing the text.
8. Finally, the Board has conducted its assessment in line with the structure foreseen in Annex 1 to the Guidelines (hereinafter "Annex"). Where this Opinion remains silent on a specific section of the BG SA's draft accreditation requirements, it should be read as the Board not having any comments and not asking the BG SA to take further action.
9. This opinion does not reflect upon items submitted by the BG SA, which are outside the scope of article 43 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

## **2.2 Main points of focus for the assessment (art. 43.2 GDPR and Annex 1 to the EDPB Guidelines) that the accreditation requirements provide for the following to be assessed consistently:**

- a. addressing all the key areas as highlighted in the Guidelines Annex and considering any deviation from the Annex.
- b. independence of the certification body
- c. conflicts of interests of the certification body
- d. expertise of the certification body
- e. appropriate safeguards to ensure GDPR certification criteria is appropriately applied by the certification body
- f. procedures for issuing, periodic review and withdrawal of GDPR certification; and
- g. transparent handling of complaints about infringements of the certification.

10. Taking into account that:

- a. Article 43 (2) GDPR provides a list of accreditation areas that a certification body needs to address in order to be accredited;

- b. Article 43 (3) GDPR provides that the requirements for accreditation of certification bodies shall be approved by the competent Supervisory Authority;
- c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for certification bodies and may decide to conduct the accreditation of certification bodies itself;
- d. Article 64 (1) (c) GDPR provides that the Board shall issue an opinion where a supervisory authority intends to approve the accreditation requirements for a certification body pursuant to Article 43(3);
- e. If accreditation is carried out by the national accreditation body in accordance with ISO/IEC 17065/2012, the additional requirements established by the competent supervisory authority must also be applied;
- f. Annex 1 of the Guidelines on Accreditation of Certification foresees suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a certification body by the National Accreditation Body;

the Board is of the opinion that:

#### 2.2.1 GENERAL REMARKS

- 11. The Board considers that in particular, it should be clear that GDPR certification is only applicable to processing operations and controllers and processors. In addition, the Board considers that the draft accreditation requirements should clearly state that the GDPR has precedence over ISO/IEC 17065/2012, as stated in the Annex. The EDPB thus encourages the BG SA to amend the requirements accordingly.
- 12. The Board notes that section “terms and definitions” states that definitions are based and in compliance with the GDPR and the relevant EDPB Guidelines. However, some of the definitions do not correspond to the definitions used for the same concepts in the GDPR and the Guidelines. Thus, it is unclear what is the relationship between some of those terms and the definitions in the GDPR and Guidelines (e.g. definition of “accreditation”). Therefore, the Board encourages the BG SA to ensure that the terms defined in the GDPR and/or the Guidelines are reflected consistently in the accreditation requirements. In addition, some terms such as “subject matter of the certification, ToE, object of evaluation, evaluation object” are used indistinctly in the draft requirements. Thus, the Board encourages the BG SA to clarify these terms and to ensure that clear and consistent wording is used thorough the document.
- 13. The Board notes that the requirements should be drafted in a prescriptive manner. Thus, the requirements should avoid the word “should” and rather use “shall” or “must”. The EDPB encourages the BG SA to make the necessary changes in this regard (e.g. in subsection 7.1.1).
- 14. In general, the Board encourages the BG SA to ensure consistency of the wording throughout the text (e.g. “Commission for Personal Data Protection”, “CPDP” or “Competent Supervisory Authority”).

## 2.2.2 GENERAL REQUIREMENTS FOR ACCREDITATION

15. Concerning subsection 4.1.1 of the BG SA's draft accreditation requirements (Legal responsibility), the Board considers that the obligation of certification bodies to have up to date procedures that demonstrate compliance with the legal responsibilities set out in the terms of accreditation should be explicitly included in the accreditation requirements. Moreover, the certification body shall be able to demonstrate evidence of GDPR compliant procedures and measures specifically for controlling and handling client organisation's personal data as part of the certification process. Therefore, the Board recommends that the BG SA amends the draft requirements accordingly.
16. Regarding point 9 of subsection 4.1.2 of the BG SA's accreditation requirements, the Board notes the inclusion of a reference to the consequences for the data subjects. However, the BG SA omitted a reference to [where applicable] "the consequences for the customer should also be addressed", as stated in the Annex. The Board therefore recommends that the BG SA replaces the term with "customer" or "client", in order to align the wording with the Annex.
17. The Board is of the opinion that point 12 of subsection 4.1.2 of the BG SA's draft accreditation requirements, regarding the obligation of the applicant to inform the certification body of infringements of the GDPR and of other data protection legislation, should be clarified. The Board considers that this obligation should not lead to self-incrimination and, therefore, the obligation should refer to infringements established by the BG SA and/or judicial authorities. Thus, the Board recommends that the BG SA makes such clarification.
18. In addition, the Board notes the obligation to lay down rules preventing conflicts of interest. The Board acknowledges the importance to have requirements that ensure, firstly, that there are no conflicts of interests and, secondly, in case conflicts of interest are identified, that the certification body manages them. Therefore, the Board encourages the BG SA to clarify that, in addition to having rules preventing conflicts, there should be clear rules to manage identified conflicts of interests.
19. With respect to subsection 4.2.3 of the BG SA's draft accreditation requirements ("Management of impartiality"), the Board encourages the BG SA to provide examples of situations where a certification body has no relevant connection with the customer it assesses. For example, the certification body should not belong to the same company group nor should be controlled in any way by the customer it assesses.
20. With regard to subsection 4.3 ("Liability and financing") of the BG SA's draft accreditation requirements, the Board notes that, in accordance with the Annex, the certification body shall demonstrate on a regular basis that it has the appropriate measures to cover its liabilities. The BG SA's draft accreditation requirements do not include the notion of "regular basis". However, since the requirement says that the measures shall cover all the validity period, the Board for sake of clarity encourages the BG SA to include directly such reference, in line with the Annex.
21. Regarding subsection 4.6.1 ("Publicly available information"), the Board recommends the BG SA to add missing element of the Annex that all certification procedures are also published and easily publicly available.
22. In addition, subsection 4.6.2 indicates that "information related to complaints on the compliance with the certification requirements, as well as, information regarding complaints on certificates' breaches, is publicly available". Which may suggest that BG SA requires the certification body to ensure that information about each individual complaint is publicly available, that is in contradiction with the Annex, which requires that at minimum information about complaints handling procedures

and appeals is made public pursuant to Article 43(2)(d). Therefore, the Board encourages the BG SA to reformulate this requirement accordingly in order to ensure that personal data included in single complaints will not be publicly available.

### 2.2.3 RESOURCE REQUIREMENTS

23. As a general remark, the Board considers that the expertise requirements for evaluators and decision-makers should be tailored taking into account the different tasks that they perform. In this regard, the Board is of the opinion that evaluators should have a more specialist expertise and professional experience in technical procedures (e.g. audits and certifications), whereas decision-makers should have a more general and comprehensive expertise and professional experience in data protection. Considering this, the Board encourages the BG SA to redraft this subsection taking into account the different substantive knowledge and/or experience requirements for evaluators and decision-makers, rather than the years of experience.
24. Regarding the educational requirements for personnel with technical expertise, the reference to a recognised protected title in the relevant regulated profession should be included. Thus, the EDPB recommends that the BG SA redrafts the requirements to clarify the above-mentioned element, in line with the Annex.
25. As regards the requirements for personnel responsible for evaluations, The Board recommends that the BG SA refers to professional experience in technical data protection as well.
26. Finally, regarding the education requirements for the technical personnel, the Board considers that the list of subjects is already tailored to the technical expertise required by the Annex. Therefore, the Board encourages the BG SA to delete the reference to “humanitarian, natural science” from the list of subjects regarding the university education of the technical personnel. In addition the Board encourages the BG SA to replace “and” by “or” before other areas.
27. According to the Annex personnel with legal expertise responsible for evaluation shall be registered as required by the Member State. Based on the explanations provided by the BG SA, the Board understands that such an obligation exists in Bulgaria. Therefore the Board recommends that the BG SA includes this requirement.
28. The Board takes note that for personnel with legal expertise “the Certification body shall use the proper procedures to ensure that the personnel specific expertise is updated taking into account the changes in the legal situation, the data protection risks and the current state of the technique and technology”. In order to avoid misunderstandings, the Board encourages the BG SA to delete word “proper”.
29. As regards section 6 point6 on representatives in the governing bodies and the individuals, who make the final decision in issuing the certificate, the Board recommends that the BG SA brings this requirement in line with the Annex by specifying “ shall have significant experiences in identifying and implementing data protection measures” instead of shall have significant professional experience in the personal data protection area.
30. In order to avoid misunderstandings, the Board encourage the BG SA to clarify the last paragraph of the section 6 of the draft accreditation requirements stating that “The above listed general requirements for the Certification body resources will be further specified in the Ordinance for the conditions and the procedure for accreditation and withdrawal of accreditation of Certification bodies, which will be adopted on the basis of these criteria”.

## 2.2.4 PROCESS REQUIREMENTS

31. In section 7 on process requirements, the Board recommends that the BG adds a reference to "*Notify the relevant CSAs before a certification body starts operating an approved European Data Protection Seal in a new Member State from a satellite office.*" so as to bring this requirement in line with the Annex.
32. The Board encourages the BG SA to redraft subsection 7.2.1. of the accreditation requirements in order to ensure consistency by using term ToE instead of "Object of certification".
33. As regards subsection 7.2 of the BG SA's accreditation requirements, the Board underlines that the applicant shall always contain a description of the data transferred to other systems or organisations, regardless of their location. Therefore, the Board encourages the BG SA to amend the wording in order to avoid confusion.
34. Regarding subsection 7.2. 2 ("Application") of the BG SA's draft accreditation requirements, the Board notes that it includes the obligation to provide "Information regarding all ongoing or closed investigations before the CPDP against the Applicant". The Board is of the opinion that the obligation should be tailored to investigations or regulatory actions related to the scope of the certification and the target of evaluation. Therefore, the Board encourages the BG SA to clarify that the investigation or regulatory action should be related to the scope of certification and the target of evaluation.
35. The Board encourages the BG SA to bring subsection 7.3.1 in line with the Annex, by adding " binding assessment methods".
36. The Board notes that the obligation to have procedures for the granting, regular review and revocation of the respective certifications pursuant to Article 43(2) and 43(3) (section 7.5 of the Annex) is not included in the BG SA's draft requirements. Thus, the Board recommends that the BG SA includes it in the requirement.
37. The Board recommends that the BG SA brings subsection 7.6 in line with subsection 7.6 of the Annex, by adding missing elements.
38. The Board notes that the second paragraph of subsection 7.6 of the BG SA's draft accreditation requirements includes the obligation to submit to the BG SA the draft decision with a summary, which should include description of the compliance with the current requirements and the certification grounds, and a declaration which states that the Applicant does not have any ongoing proceeding before CPDP, prior to issuing, renewing or validity extension of the certification. Based on the explanations provided by the BG SA, the Board understands that the intention of this requirement is to increase transparency and it does not entail a supervision of the draft approval. The Board encourages the BG SA to include a clarification in that sense.
39. With regard to subsection 7.7 ("Certification documentation"), the Board notes that the BG SA's accreditation requirements do not include the last paragraph of section 7.7 of the Annex. The Board considers that these requirements should be in the text of the accreditation requirements and recommends that the BG SA amends the requirements in order to include the information.
40. In subsection 7.8 point 1 the Board recommends that the BG SA adds a meaningful description on the object of certification pursuant to the Guidelines.
41. The Board encourages the BG SA to add in section 7.8 point 2 the phrase "including version or functional status".

42. In addition the Board recommends that the BG SA clarifies in line with section 7.8 of the Annex that elements listed in subsection 7.8 (points 1-4) are part of the executive summary and must be publicly available.
43. With regard to the last sentence of subsection 7.8 of the BG SA's draft accreditation requirements, the Board notes that this section concerns the obligation to inform the CPDP upon request of the reasons for issuance or non-issuance of a certificate, whereas the requirement in subsection 7.8 of the Annex to the Guidelines contains an obligation to proactively inform the SA of the reasons for granting or revoking the certification. Therefore, the Board recommends that the BG SA amends the draft accordingly.
44. With regard to subsection 7.9 of the BG SA's draft accreditation requirements ("Surveillance"), the Board considers that the risks associated with the processing should be taken into account in order to determine how frequent monitoring is necessary. Therefore, the Board encourages the BG SA to include a risk-based approach with regard to the arrangements for surveillance.
45. With regard to subsection 7.10 of the BG SA's draft accreditation requirements ("changes affecting certification"), the Board considers that changes in the state of art are also relevant and might affect certification. Therefore, the Board encourages the BG SA to include this possibility among the list of changes that might affect certification.
46. In addition, the Board notes that subsection 7.10 includes "data security breaches or data protection legislation infringements". The Board considers that, in order to avoid self-incrimination, the reference should be to infringements established by the BG SA or the competent judicial authority. Therefore, the Board encourages the BG SA to add the abovementioned reference. At the same time, in order to ensure clarity, the Board encourages the BG SA to specify that the data security breaches or data protection legislation infringements shall be taken into account only inasmuch as they relate to the certification.
47. Additionally, the Board observes that there is no reference to the change procedures to be agreed, as per subsection 7.10 of the Annex. The Board encourages the BG SA to include such reference and mention some of the procedures that could be put in place (e.g. transition periods, approvals process with the competent SA...).
48. Regarding the obligation to inform the BG SA of the reasons for the termination, reduction, suspension or withdrawal of a certification (subsection 7.11 of the BG SA's accreditation requirements), the Board encourages the BG SA to clarify that the information should be provided in writing.
49. In subsection 7.12, the Board recommends that the BG SA specify that the certification body should be required to keep all documentation complete, comprehensible, up-to-date and fit to audit in line with subsection 7.12 of the Annex.
50. In subsection 7.13 ("Complaints and appeals, Art. 43 (2) (d)'), the Board recommends that the BG SA adds the missing elements of subsection 7.13 of the Annex such as "how and to whom such confirmation must be given" and "which processes are to be initiated afterwards".

## 2.2.5 MANAGEMENT SYSTEM REQUIREMENTS

51. The Board understands that section 8 of the BG SA's draft accreditation requirements includes the obligation to disclose to the BG SA the management principles and their documented implementation during the accreditation procedure and, afterwards, at the request of the BG SA at any time during an investigation, as stated in the Annex. However wording of this section is not fully in line with paragraph

4 and 5, section 8 of the Annex. Therefore, the Board recommends that the BG SA brings this section fully in line with the Annex.

## 2.2.6 FURTHER ADDITIONAL REQUIREMENTS

52. The first sentence of subsection 9.1 (“Updating of evaluation methods”) of the BG SA’s draft accreditation requirements refers to “the context of evaluation under point 7.4 of ISO/IEC 17065/2012”, which does not reflect the wording of subsection 9.1 of the Annex. Therefore, the Board recommends that the BG SA adds the reference to the evaluation under subsection 7.4 of the BG SA’s accreditation requirements.
53. The Board considers that subsection 9.3.4 of the BG SA’s draft accreditation requirements is not in line with subsection 9.3.4 of the Annex, in particular the reference to notification to customers in the event of suspension or withdrawal of the accreditation is missing. The Board recommends that the BG SA includes the missing elements, in line with the Annex.

## 3 CONCLUSIONS / RECOMMENDATIONS

54. The draft accreditation requirements of the Bulgarian Supervisory Authority may lead to an inconsistent application of the accreditation of certification bodies and the following changes need to be made:
  55. Regarding ‘general requirements for accreditation’, the Board recommends that the BG SA:
    - 1) amends subsection 4.1.1 of the BG SA’s draft accreditation requirements in order to ensure that the obligation of certification bodies to have up to date procedures that demonstrate compliance with the legal responsibilities set out in the terms of accreditation should be explicitly included in the accreditation requirements as well as the certification body shall be able to demonstrate evidence of GDPR compliant procedures and measures specifically for controlling and handling client organisation’s personal data as part of the certification process.
    - 2) replaces in point 9 of subsection 4.1.2 of the BG SA’s accreditation requirements the term “data subject” with the term “customer”, in order to align the wording with the Annex.
    - 3) makes clarification in point 12 of subsection 4.1.2 of the BG SA’s draft accreditation requirements that the obligation of the applicant to inform the certification body of infringements of the GDPR should refer to infringements established by the BG SA and/or judicial authorities.
    - 4) adds in subsection 4.6.1 missing element of the Annex that all certification procedures are also published and easily publicly available.
    - 5) adds in subsection 4.6.2 that information about complaints handling procedures and appeals is made public pursuant to Article 43(2)(d).
  56. Regarding ‘resource requirements’, the Board recommends that the BG SA:
    - 1) adds a reference to a recognised protected title in the relevant regulated profession into the education requirements for personnel with technical expertise in line with the Annex.

- 2) refers in the requirements for personnel responsible for evaluations to professional experience in technical data protection as well.
- 3) includes to the requirements that personnel with legal expertise responsible for evaluation shall be registered as required by BG law.
- 4) specifies in section 6 point 6 that representatives in the governing bodies and the individuals, who make the final decision in issuing the certificate "shall have significant experiences in identifying and implementing data protection measures".

57. Regarding 'process requirements', the Board recommends that the BG SA:

- 1) adds in section 7 a reference to "Notify the relevant CSAs before a certification body starts operating an approved European Data Protection Seal in a new Member State from a satellite office."
- 2) includes the obligation to have procedures for the granting, regular review and revocation of the respective certifications pursuant to Article 43(2) and 43(3) (subsection 7.5 Annex).
- 3) brings subsection 7.6 in line with subsection 7.6 of the Annex, by adding missing elements.
- 4) adds in subsection 7.7 ("Certification documentation") the last paragraph of section 7.7 of the Annex.
- 5) adds in subsection 7.8. point 1) "a meaningful description" on the object of certification pursuant to the Guidelines.
- 6) clarifies in line with subsection 7.8 of the Annex that elements listed in subsection 7.8 (points 1-4) are part of the executive summary and must be publicly available.
- 7) amends the last sentence of subsection 7.8 of the BG SA's draft accreditation requirements, that certification body is obliged to proactively inform the SA of the reasons for granting or revoking the certification.
- 8) specifies in subsection 7.12 that the certification body should be required to keep all documentation complete, comprehensible, up-to-date and fit to audit in line with subsection 7.12 of the Annex.
- 9) adds in subsection 7.13 missing elements of section 7.13 of the Annex such as "how and to whom such confirmation must be given" and "which processes are to be initiated afterwards".

58. Regarding 'management system requirements', the Board recommends that the BG SA:

- 1) brings section 8 fully in line with paragraph 4 and 5, section 8 of the Annex.

59. Regarding 'further additional requirements', the Board recommends that the BG SA:

- 1) adds a reference to the evaluation under subsection 7.4 of the BG SA's accreditation requirements in line with the wording of subsection 9.1. of the Annex.
  - 2) includes in the subsection 9.3.4 of the BG SA's draft accreditation requirement reference to notification to customers in the event of suspension or withdrawal of the accreditation.
- Final Remarks

## 4 FINAL REMARKS

60. This opinion is addressed to the Bulgarian Supervisory Authority and will be made public pursuant to Article 64 (5)(b) GDPR.
61. According to Article 64 (7) and (8) GDPR, the BG SA shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.
62. The BG SA shall communicate the final decision to the Board for inclusion in the register of decisions, which have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

# Opinion of the Board (Art. 64)



**Opinion 14/2022 on the draft decision of the competent supervisory authority of Bulgaria regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR**

**Adopted on 4 July 2022**

## Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT .....	4
2.1	General reasoning of the Board regarding the submitted draft accreditation requirements.	4
2.2	Analysis of the BG SA's accreditation requirements for Code of Conduct's monitoring bodies	5
2.2.1	GENERAL REMARKS .....	5
2.2.2	CONFLICT OF INTEREST .....	7
2.2.3	EXPERTISE .....	7
2.2.4	ESTABLISHED PROCEDURES AND STRUCTURES.....	8
2.2.5	TRANSPARENT COMPLAINT HANDLING .....	8
2.2.6	COMMUNICATION WITH THE BG SA .....	8
2.2.7	REVIEW MECHANISMS .....	8
3	CONCLUSIONS / RECOMMENDATIONS .....	9
4	FINAL REMARKS.....	9

## **The European Data Protection Board**

Having regard to Article 63, Article 64 (1)(c), (3)-(8) and Article 41 (3) 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 10 and Article 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the European Data Protection Board (hereinafter “the Board”) is to ensure the consistent application of the GDPR when a supervisory authority (hereinafter “SA”) intends to approve the requirements for accreditation of a code of conduct (hereinafter “code”) monitoring body pursuant to article 41. The aim of this opinion is therefore to contribute to a harmonised approach with regard to the suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a code monitoring body by the competent supervisory authority. Even though the GDPR does not directly impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinion by: firstly, requesting the competent SAs to draft their requirements for accreditation of monitoring bodies based on article 41(2) GDPR and on the Board’s “Guidelines 1/2019 on Codes of Conduct and Monitoring bodies under Regulation 2016/679” (hereinafter the “Guidelines”), using the eight requirements as outlined in the guidelines’ accreditation section (section 12); secondly, providing the competent SAs with written guidance explaining the accreditation requirements; and, finally, requesting the competent SAs to adopt the requirements in line with this opinion, so as to achieve a harmonised approach.

(2) With reference to article 41 GDPR, the competent supervisory authorities shall adopt requirements for accreditation of monitoring bodies of approved codes. They shall, however, apply the consistency mechanism in order to allow the setting of suitable requirements ensuring that monitoring bodies carry out the monitoring of compliance with codes in a competent, consistent and independent manner, thereby facilitating the proper implementation of codes across the Union and, as a result, contributing to the proper application of the GDPR.

(3) In order for a code covering non-public authorities and bodies to be approved, a monitoring body (or bodies) must be identified as part of the code and accredited by the competent SA as being capable of effectively monitoring the code. The GDPR does not define the term “accreditation”. However, article 41 (2) of the GDPR outlines general requirements for the accreditation of the monitoring body. There are a number of requirements, which should be met in order to satisfy the competent supervisory authority to accredit a monitoring body. Code owners are required to explain and

---

<sup>1</sup> References to the “Union” made throughout this opinion should be understood as references to “EEA”.

demonstrate how their proposed monitoring body meets the requirements set out in article 41 (2) GDPR to obtain accreditation.

(4) While the requirements for accreditation of monitoring bodies are subject to the consistency mechanism, the development of the accreditation requirements foreseen in the Guidelines should take into consideration the code's sector or specificities. Competent supervisory authorities have discretion with regard to the scope and specificities of each code, and should take into account their relevant legislation. The aim of the Board's opinion is therefore to avoid significant inconsistencies that may affect the performance of monitoring bodies and consequently the reputation of GDPR codes of conduct and their monitoring bodies.

(5) In this respect, the Guidelines adopted by the Board will serve as a guiding thread in the context of the consistency mechanism. Notably, in the Guidelines, the Board has clarified that even though the accreditation of a monitoring body applies only for a specific code, a monitoring body may be accredited for more than one code, provided it satisfies the requirements for accreditation for each code.

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

#### **HAS ADOPTED THE FOLLOWING OPINION:**

## **1 SUMMARY OF THE FACTS**

1. The Bulgarian Supervisory Authority (hereinafter "BG SA") has submitted its draft decision containing the accreditation requirements for a code of conduct monitoring body to the Board, requesting its opinion pursuant to article 64 (1)(c), for a consistent approach at Union level. The decision on the completeness of the file was taken on 28 March 2022.

## **2 ASSESSMENT**

### **2.1 General reasoning of the Board regarding the submitted draft accreditation requirements**

2. All accreditation requirements submitted to the Board for an opinion must fully address article 41 (2) GDPR criteria and should be in line with the eight areas outlined by the Board in the accreditation section of the Guidelines (section 12, pages 21-25). The Board opinion aims at ensuring consistency and a correct application of article 41 (2) GDPR as regards the presented draft.
3. This means that, when drafting the requirements for the accreditation of a body for monitoring codes according to articles 41 (3) and 57 (1) (p) GDPR, all the SAs should cover these basic core requirements foreseen in the Guidelines, and the Board may recommend that the SAs amend their drafts accordingly to ensure consistency.

4. All codes covering non-public authorities and bodies are required to have accredited monitoring bodies. The GDPR expressly request SAs, the Board and the Commission to “encourage the drawing up of codes of conduct intended to contribute to the proper application of the GDPR, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium sized enterprises.” (article 40 (1) GDPR). Therefore, the Board recognises that the requirements need to work for different types of codes, applying to sectors of diverse size, addressing various interests at stake and covering processing activities with different levels of risk.
5. In some areas, the Board will support the development of harmonised requirements by encouraging the SA to consider the examples provided for clarification purposes.
6. When this opinion remains silent on a specific requirement, it means that the Board is not asking the BG SA to take further action.
7. This opinion does not reflect upon items submitted by the BG SA, which are outside the scope of article 41 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

## 2.2 Analysis of the BG SA’s accreditation requirements for Code of Conduct’s monitoring bodies

8. Taking into account that:
  - a. Article 41 (2) GDPR provides a list of accreditation areas that a monitoring body need to address in order to be accredited;
  - b. Article 41 (4) GDPR requires that all codes (excluding those covering public authorities per Article 41 (6)) have an accredited monitoring body; and
  - c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for monitoring bodies and conduct the accreditation of a body for monitoring codes of conduct.

the Board is of the opinion that:

### 2.2.1 GENERAL REMARKS

9. For the sake of consistency and clarity, the Board encourages the BG SA to replace throughout the draft accreditation requirements the term “Commission for Personal Data Protection” or “CPDP” with the term “Competent Supervisory Authority” in line with the terminology used in the Guidelines. At the same time the Board encourages the BG SA to introduce in the draft requirements a definition of the term «Competent Supervisory Authority», to be understood as the Commission for Personal Data Protection.
10. In general, the Board encourages the BG SA to ensure consistency of the wording throughout the text. For instance in paragraph 4, chapter I, the term “candidate for accreditation” is introduced instead of the accreditation applicant. In paragraph 9, chapter I, section 1; paragraph 13, chapter I, section 3; paragraph 24, chapter II and paragraph 31, chapter IV, the pronouns ‘his/her’, ‘him/her’ are used instead of ‘its’ or ‘it’ with regards to the accreditation applicant .

11. In addition, the Board encourages the BG SA to complete the text with the missing words where needed (e.g. in section 1, chapter I insert the verb “shall” and in the first sentence of paragraph 12, the verb “must”).
12. The Board observes that the last paragraph on page 1 of the introductory chapter and chapter IX (paragraphs 44 to 46) of the BG SA’s draft accreditation requirements refer to a monitoring body of a code of conduct as a tool for international transfers. The Board adopted on 22 February 2022 “the Guidelines 04/2021 on Codes of Conduct as tools for transfers”. In the opinion of the Board, the Guidelines 04/2021 do not add any additional requirements for the accreditation of monitoring bodies that monitor codes of conduct intended for international transfers. Rather, the Guidelines 04/2021 provide further specifications of the general requirements established by the Guidelines 1/2019 (Section 12) taking into account the specific context of international transfers<sup>2</sup>. Therefore, the Board recommends that the BG SA deletes paragraphs 44 and 46 and add paragraph 45 according to which “the code of conduct serving as a data transfer mechanism may also include additional specific requirements for the monitoring body to be fulfilled at the time of accreditation” in the introductory chapter, along with a general reference to the Guidelines 04/2021.

### 13. INDEPENDENCE

14. In section 1, chapter I («Legal and decision making procedure») of the BG SA’s draft accreditation requirements, the Board encourages the BG SA to clarify the sentence “the nature of the decisions taken” included the examples provided under paragraph 7.
15. As for section 2, chapter I (« Financial independence») of the BG SA’s draft accreditation requirements, the Board acknowledges that monitoring bodies should be provided with the financial stability and necessary resources for the effective and independent performance of their tasks. The means by which a monitoring body receives financial support should not adversely affect the independence of its task of monitoring compliance of a code. The funding of the monitoring body and the transparency of such funding constitute a decisive element to assess the independence of the monitoring body. For this reason, the Board recommends that the BG SA replaces “should” by “must” or “shall” and add the word ‘independently’ in the first sentence of this section which refers to the need for the monitoring body to demonstrate having “sufficient financial resources to carry out effectively the tasks and responsibilities referred to in Article 41(1) of Regulation (EU) 2016/679”.
16. With regard to the financial independence (paragraph 10), in the opinion of the Board, the monitoring body would not be considered financially independent if the rules governing its financial support allow a code member, who is under investigation by the monitoring body, to stop its financial contributions to it, in order to avoid a potential sanction from the monitoring body. Therefore, the Board encourages the BG SA to elaborate further this requirement by providing more examples of how the monitoring body can provide such evidence.
17. With regard to paragraph 11 of section 3 («Legal status and organisational independence»), for the sake of clarity the Board encourages the BG SA to redraft the last part of the second sentence stating that the monitoring body can act as an internal or external monitoring body vis-à-vis the code owner, “with the choice of a particular approach at the discretion of the code owner”.

---

<sup>2</sup> See Section4.2 of the EDPB Guidelines 04/2021 on Codes of Conduct as tools for transfers.

18. Regarding paragraph 12 on internal monitoring bodies, the Board recommends the BG SA to add a requirement to prove that the internal monitoring body has a specific separated budget that is able to manage independently.
19. With regard to paragraph 14 of the BG SA's draft accreditation requirements devoted to the assessment of the structuring of an internal monitoring body, the Board takes note that the second sentence at the end contains the phrase "falling within its scope" and for the sake of clarity, encourages the BG SA to clarify that this sentence, by referring expressly to the scope of the code of conduct.
20. With respect to paragraph 15, addressing the need for the monitoring body to prove, among others, that it has "adequate" human resources for the effective performance of its functions under Article 41(1) of Regulation (EU) 2016/679, the Board encourages BG SA to consider making a reference to "sufficient numbers of sufficiently qualified personnel".
21. As regards paragraph 17 of the BG SA's accreditation requirements, the Board understands that, read together with paragraph 19, it establishes that the monitoring body is always the ultimate responsible for the decision-making and for compliance with its obligations, also when it uses subcontractors. The Board encourages the BG SA to clarify the wording as above.
22. In addition, in paragraph 17, the Board recommends that the BG SA adds a clear indication that the monitoring body shall ensure effective monitoring of the services provided by subcontractors.

### **2.2.2 CONFLICT OF INTEREST**

23. With regard to chapter II of the BG SA's draft accreditation requirements, the Board encourages the BG SA to clarify that the phrase "persons employed by it outside its structure" in the first sentence of paragraph 23 includes both natural and legal persons such as subcontractors.
24. As for the second sentence in paragraph 23 which reads "Any interest that results in an advantage of a tangible or intangible nature and/or in the impartial and objective performance of the duties and functions referred to in Article 41(1) of the Regulation is private", the Board notes that the last part of this sentence does not adequately convey the meaning of private interests, as a conflict of interest can be said to arise when it affects the impartial and objective performance of the monitoring body's duties and functions. Therefore, the Board recommends the BG SA to reformulate the sentence as follows "Any interest that results in an advantage of a tangible or intangible nature and/or in affecting the impartial and objective performance of the duties and functions referred to in Article 41(1) of the Regulation is private".

### **2.2.3 EXPERTISE**

25. As regards chapter III, paragraph 26 of the BG SA's draft accreditation requirements, the Board encourages the BG SA to add also a reference to the "knowledge" alongside the "appropriate expertise" in data protection law with respect to the monitoring body's personnel performing decision-making functions.
26. Whilst the BG SA has included all the elements from the Guidelines in these requirements devoted to the expertise of the monitoring body, the Board is of the opinion that the level of the knowledge and expertise in data protection issues should be aligned with the Guidelines. Therefore, the Board encourages the BG SA to align the text with the Guidelines, and require an "in-depth" understanding of data protection legislation.

#### **2.2.4 ESTABLISHED PROCEDURES AND STRUCTURES**

27. With regard to paragraph 31, chapter IV, of the BG SA's accreditation requirements («Structures, resources and established procedures for the monitoring of a code of conduct»), the Board encourages the BG SA to clarify that the human resources of the monitoring body must be appropriate to the expected number and size of code members, as well as the complexity or degree of risk of the relevant data processing in line with section 73 of the Guidelines.

#### **2.2.5 TRANSPARENT COMPLAINT HANDLING**

28. Regarding paragraph 36, chapter V, of the BG SA's draft accreditation requirements, the Board considers that under section 74 of the Guidelines, the requirements related to the complaint handling process must contain the obligation of the monitoring body to make its decisions or general information thereof, publicly available. Therefore, the Board recommends that the requirement is redrafted accordingly. In addition, the Board encourages the BG SA to clarify that information on the complaint handling process must be publicly accessible.

#### **2.2.6 COMMUNICATION WITH THE BG SA**

29. The Board notes that the BG SA's accreditation requirements, chapter VI, provides for annual reporting by the monitoring body to the BG SA. The Board encourages the BG SA to require more regular communication means towards the BG SA during the year in paragraph 40. The Board is of the opinion that the requirements need to address, in particular, such areas as: actions taken in cases of infringement of the code and the reasons for taking them (Article 41 (4) GDPR), periodic reports, reviews or audit findings. The code itself will also outline the communication requirements with the BG SA, including appropriate ad hoc and regular reports. In the case of serious infringements of the code by code members, which result in serious actions such as suspension or exclusion from the code, the BG SA should be informed without undue delay, in line with paragraph 77 of the Guidelines.

#### **2.2.7 REVIEW MECHANISMS**

30. The Board observes that, in paragraph 41 of the BG SA's draft accreditation requirements, it is stated that need for change or update of the code of conduct "may arise, for example, in the event of a change in the applicable legislation or in order to take account of the latest technological developments". In line with the Guidelines, the review mechanisms should take also into account any changes in the application and interpretation of the law which have impact upon the data processing carried out by the code members or the provisions of the code. Therefore, the Board encourages the BG SA to appropriately enrich this requirement.
31. With regard to paragraph 42, the Board notes the reference to the review and "ex-post evaluation" of the relevant part of the code. In order to avoid misunderstandings, the Board encourages the BG SA to delete "ex-post".
32. The Board observes that data security obligations may not be included in the scope of a Code of Conduct (e.g. a Code of Conduct may be focused only on transparency toward data subjects). Therefore, the Board encourages the BG SA to add "If applicable" in paragraph 42, second indent, concerning the information on personal data breaches to be provided to the code owner by the monitoring body in the context of the procedure aimed at reviewing periodically the code of conduct.

### 3 CONCLUSIONS / RECOMMENDATIONS

33. The draft accreditation requirements of the BG Supervisory Authority may lead to an inconsistent application of the accreditation of monitoring bodies and the following changes need to be made:
34. Regarding *general remarks* the Board recommends that the BG SA:
  1. deletes paragraphs 44 and 46 and add paragraph 45, according to which “The code of conduct serving as a data transfer mechanism may also include additional specific requirements for the monitoring body to be fulfilled at the time of accreditation” in the introductory chapter, along with a general reference to the Guidelines 04/2021.
35. Regarding *independence* the Board recommends that the BG SA:
  1. replaces “should” by “must” or “shall” and add the word “independently” in the first sentence of section 2, which refers to the need for the monitoring body to demonstrate having “sufficient financial resources to carry out effectively the tasks and responsibilities of referred to in Article 41(1) of Regulation (EU) 2016/679”;
  2. Regarding paragraph 12 on internal monitoring bodies, the Board recommends the BG SA to adds a requirement to prove that the internal monitoring body has a specific separated budget;
  3. adds in paragraph 17 a clear indication that the monitoring body shall ensure effective monitoring of the services provided by subcontractors.
36. Regarding *conflict of interest* the Board recommends that the BG SA:
  1. reformulates the second sentence in paragraph 23 as follows ”Any interest that results in an advantage of a tangible or intangible nature and/or in affecting the impartial and objective performance of the duties and functions referred to in Article 41(1) of the Regulation is private”.
37. Regarding *transparent complaint handling* the Board recommends that the BG SA:
  1. redrafts paragraph 36 to include an obligation for the monitoring body to make its decisions or general information about them publicly available.

### 4 FINAL REMARKS

38. This opinion is addressed to the Bulgarian supervisory authority and will be made public pursuant to Article 64 (5) (b) GDPR.
39. According to Article 64 (7) and (8) GDPR, the BG SA shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft decision. Within the same period, it shall provide the amended draft decision or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.
40. The BG SA shall communicate the final decision to the Board for inclusion in the register of decisions, which have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

# Opinion of the Board (Art. 64)



**Opinion 15/2022 on the draft decision of the competent supervisory authority of Luxembourg regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR**

**Adopted on 4 July 2022**

## Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT .....	4
2.1	General reasoning of the Board regarding the submitted draft accreditation requirements.	4
2.2	Analysis of the LU SA's accreditation requirements for Code of Conduct's monitoring bodies	
	5	
2.2.1	GENERAL REMARKS .....	5
2.2.2	INDEPENDENCE .....	6
2.2.3	CONFLICT OF INTEREST .....	7
2.2.4	EXPERTISE .....	7
2.2.5	ESTABLISHED PROCEDURES AND STRUCTURES.....	8
2.2.6	TRANSPARENT COMPLAINT HANDLING .....	8
2.2.7	COMMUNICATION WITH THE LU SA .....	8
2.2.8	REVIEW MECHANISMS .....	8
2.2.9	LEGAL STATUS .....	8
3	CONCLUSIONS / RECOMMENDATIONS .....	9
4	FINAL REMARKS.....	10

## **The European Data Protection Board**

Having regard to Article 63, Article 64 (1)(c), (3)-(8) and Article 41 (3) 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 10 and Article 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the European Data Protection Board (hereinafter “the Board”) is to ensure the consistent application of the GDPR when a supervisory authority (hereinafter “SA”) intends to approve the requirements for accreditation of a code of conduct (hereinafter “code”) monitoring body pursuant to article 41. The aim of this opinion is therefore to contribute to a harmonised approach with regard to the suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a code monitoring body by the competent supervisory authority. Even though the GDPR does not directly impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinion by: firstly, requesting the competent SAs to draft their requirements for accreditation of monitoring bodies based on article 41(2) GDPR and on the Board’s “Guidelines 1/2019 on Codes of Conduct and Monitoring bodies under Regulation 2016/679” (hereinafter the “Guidelines”), using the eight requirements as outlined in the guidelines’ accreditation section (section 12); secondly, providing the competent SAs with written guidance explaining the accreditation requirements; and, finally, requesting the competent SAs to adopt the requirements in line with this opinion, so as to achieve an harmonised approach.

(2) With reference to article 41 GDPR, the competent supervisory authorities shall adopt requirements for accreditation of monitoring bodies of approved codes. They shall, however, apply the consistency mechanism in order to allow the setting of suitable requirements ensuring that monitoring bodies carry out the monitoring of compliance with codes in a competent, consistent and independent manner, thereby facilitating the proper implementation of codes across the Union and, as a result, contributing to the proper application of the GDPR.

(3) In order for a code covering non-public authorities and bodies to be approved, a monitoring body (or bodies) must be identified as part of the code and accredited by the competent SA as being capable of effectively monitoring the code. The GDPR does not define the term “accreditation”. However, article 41 (2) of the GDPR outlines general requirements for the accreditation of the monitoring body. There are a number of requirements, which should be met in order to satisfy the competent supervisory authority to accredit a monitoring body. Code owners are required to explain and

---

<sup>1</sup> References to the “Union” made throughout this opinion should be understood as references to “EEA”.

demonstrate how their proposed monitoring body meets the requirements set out in article 41 (2) GDPR to obtain accreditation.

(4) While the requirements for accreditation of monitoring bodies are subject to the consistency mechanism, the development of the accreditation requirements foreseen in the Guidelines should take into consideration the code's sector or specificities. Competent supervisory authorities have discretion with regard to the scope and specificities of each code, and should take into account their relevant legislation. The aim of the Board's opinion is therefore to avoid significant inconsistencies that may affect the performance of monitoring bodies and consequently the reputation of GDPR codes of conduct and their monitoring bodies.

(5) In this respect, the Guidelines adopted by the Board will serve as a guiding thread in the context of the consistency mechanism. Notably, in the Guidelines, the Board has clarified that even though the accreditation of a monitoring body applies only for a specific code, a monitoring body may be accredited for more than one code, provided it satisfies the requirements for accreditation for each code.

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

#### **HAS ADOPTED THE FOLLOWING OPINION:**

## **1 SUMMARY OF THE FACTS**

1. The Luxembourg Supervisory Authority (hereinafter "LU SA") has submitted its draft decision containing the accreditation requirements for a code of conduct monitoring body to the Board, requesting its opinion pursuant to article 64 (1)(c), for a consistent approach at Union level. The decision on the completeness of the file was taken on 28 March 2022.

## **2 ASSESSMENT**

- 2.1 General reasoning of the Board regarding the submitted draft accreditation requirements**
2. All accreditation requirements submitted to the Board for an opinion must fully address article 41 (2) GDPR criteria and should be in line with the eight areas outlined by the Board in the accreditation section of the Guidelines (section 12, pages 21-25). The Board opinion aims at ensuring consistency and a correct application of article 41 (2) GDPR as regards the presented draft.
3. This means that, when drafting the requirements for the accreditation of a body for monitoring codes according to articles 41 (3) and 57 (1) (p) GDPR, all the SAs should cover these basic core requirements foreseen in the Guidelines, and the Board may recommend that the SAs amend their drafts accordingly to ensure consistency.

4. All codes covering non-public authorities and bodies are required to have accredited monitoring bodies. The GDPR expressly request SAs, the Board and the Commission to “encourage the drawing up of codes of conduct intended to contribute to the proper application of the GDPR, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium sized enterprises.” (article 40 (1) GDPR). Therefore, the Board recognises that the requirements need to work for different types of codes, applying to sectors of diverse size, addressing various interests at stake and covering processing activities with different levels of risk.
5. In some areas, the Board will support the development of harmonised requirements by encouraging the SA to consider the examples provided for clarification purposes.
6. When this opinion remains silent on a specific requirement, it means that the Board is not asking the LU SA to take further action.
7. This opinion does not reflect upon items submitted by the LU SA, which are outside the scope of article 41 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

## 2.2 Analysis of the LU SA's accreditation requirements for Code of Conduct's monitoring bodies

8. Taking into account that:
  - a. Article 41 (2) GDPR provides a list of accreditation areas that a monitoring body need to address in order to be accredited;
  - b. Article 41 (4) GDPR requires that all codes (excluding those covering public authorities per Article 41 (6)) have an accredited monitoring body; and
  - c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for monitoring bodies and conduct the accreditation of a body for monitoring codes of conduct.

the Board is of the opinion that:

### 2.2.1 GENERAL REMARKS

9. The Board notes that on 22 February 2022, “the Guidelines 04/2021 on Codes of Conduct as tools for transfers” were adopted. These guidelines do not add any additional requirements for the accreditation of monitoring bodies that monitor codes of conduct intended for international transfers. Rather, the guidelines provide further specifications of the general requirements established by the Guidelines 1/2019 (Section 12) taking into account the specific context of international transfers<sup>2</sup>. For the sake of clarity, the Board recommends the LU SA to add a reference to the above-mentioned guidelines, which are relevant in the context of monitoring codes of conduct intended for international transfers.

---

<sup>2</sup> See Section4.2 of the EDPB Guidelines 04/2021 on Codes of Conduct as tools for transfers

10. The Board encourages the LU SA to include either in the draft accreditation requirements or in the complementary guidance to the requirements, some examples of the information or documents that applicants have to submit when applying for accreditation.
11. The Board notes that the requirements state that an internal monitoring body “could be an internal department within the code owner”. The Board considers that it should be made explicit that an internal monitoring body cannot be setup within a code member. Therefore, the Board recommends adding a relevant provision.
12. The Board notes that there is no reference to the duration of the accreditation or accreditation withdrawal procedures. Whilst the Board accepts that these areas fall into the area of guidance supporting the accreditation requirements, the Board considers them important areas in terms of ensuring that the whole accreditation process is transparent. On the basis of the explanations provided by the LU SA, the Board understands that the information will be included in the accreditation procedure, and welcomes such inclusion.
13. The Board observes that the LU SA’s draft accreditation requirements are sometimes worded in present tense, instead of as an obligation (e.g. sections 5.5 and 6.1). For the sake of clarity, the Board recommends that the LU SA formulate the requirements as an obligation (ie. using “shall”, “must”, or equivalent term).
14. The Board observes that the draft requirements make several references to “audit”, instead of “monitoring”. Based on the explanations provided by the LU SA, the Board understands that “audit” is used as a synonym of “monitoring”. However, in order to avoid confusion, the Board encourages the LU SA to make it clearer.

### 2.2.2 INDEPENDENCE

15. The Board welcomes the inclusion of explanatory notes in the LU SA’s draft accreditation requirements, as they contribute to improve the clarity and understanding thereof.
16. The Board considers that the requirements concerning the organisational and financial independence of the monitoring body (section 1.4 and 1.7 of the draft requirements, respectively) should address the boundary conditions that determine the concrete requirements. These include the expected number, size and complexity of the code members (as monitored entities), the nature and scope of their activities (which are the subject of the code) and the complexity or degree of risk(s) of the relevant processing operation(s). Therefore, the Board encourages the LU SA to redraft the requirements accordingly.
17. Moreover, with regard to the organisational resources (section 1.4), the Board observes that the draft accreditation requirements refer to “adequate resources and personnel to effectively perform its task”. The Board encourages LU SA to redraft the relevant part of the requirements by adding a reference to “sufficient number of sufficiently qualified personnel” and including a reference to technical resources necessary for the effective performance of the monitoring body’s task.
18. In addition, the Board considers that the requirements on financial resources would benefit from the inclusion of some examples with regard to the financial independence of the monitoring body, in order to highlight how the monitoring body can demonstrate that the means by which it obtains financial support should not adversely affect its independence (section 1.7). For instance, the monitoring body would not be considered financially independent if the rules governing its financial support allow a code member, who is under investigation by the monitoring body, to stop its financial contributions to

it, in order to avoid a potential sanction from the monitoring body. The Board encourages the LU SA to such clarification and provide examples of how the monitoring body can provide such evidence.

19. Regarding section 1.5 on internal monitoring bodies, the Board considers that the impartiality of the internal monitoring body shall be ensured not only towards the larger entity, but towards the overall group structure. The Board encourages the LU SA to make the necessary amendments.
20. In addition, the Board underlines that, according to point 65 of the Guidelines, where an internal monitoring body is proposed, there should be separate personnel and management, accountability and function from other areas of the organisation. The LU SA's draft accreditation requirements do not include a reference to a separate accountability and, therefore, the Board recommends to add such reference. Likewise, the Board recommends the LU SA to add a requirement to prove that the internal monitoring body has a specific separated budget that is able to manage independently.

#### **2.2.3 CONFLICT OF INTEREST**

21. As a general remark in this section, the Board is of the opinion that, for practical reasons, more detailed examples of cases where a conflict of interest could arise might be helpful. An example of a conflict of interest situation would be the case where personnel conducting audits or making decisions on behalf of a monitoring body had previously worked for the code owner, or for any of the organisations adhering to the code. Therefore, the Board encourages the LU SA to elaborate on the examples included in the explanatory note.
22. Furthermore, the Board observes that the LU SA accreditation requirements do not explicitly include the obligation of the monitoring body to refrain from any action that is incompatible with its tasks and duties (paragraph 68, page 23 of the Guidelines). Therefore, the Board recommends the LU SA to align the text with the Guidelines and include the above-mentioned obligation.

#### **2.2.4 EXPERTISE**

23. The EDPB welcomes the explanations provided in the explanatory note and encourages the LU SA to include some addition examples of documentation that demonstrates the necessary experience, such as data protection certifications and training certificates.
24. With regard to section 3.5, the Board notes that it distinguishes 3 types of personnel: auditors, "other technical experts", legal experts. However, it is unclear what is the difference between the three types of personnel. In addition, point b) seems to imply that auditors are technical personnel. The Board considers that this curtails the possibility for legal personnel to perform audits. Therefore, the Board recommends the LU SA to clarify the differences between the three roles and ensure consistency in the requirements, in order to not curtail the freedom of the code owner to define the type of expertise required for each role.
25. Furthermore, the EDPB considers that the requirements for the personnel are very specific and may curtail the freedom of the code owner to define the specific expertise requirements in the code of conduct. The Board encourages the LU SA to make the requirements less restrictive by including a more general reference that takes into account the different types of codes, such as "a relevant level of experience in accordance with the code itself".
26. In addition, the Board observes that the LU SA makes a distinction between legal and technical personnel. The Board encourages the LU SA to clarify that the technical requirements of the personnel will depend on whether it is necessary for the code at stake.

### 2.2.5 ESTABLISHED PROCEDURES AND STRUCTURES

27. With regard to section 4.5, the Board notes that the procedure to ensure the monitoring of the code of conduct will take into account the “number of code members”. Since the number of code members may not be known at the moment the monitoring body applies for accreditation, the Board encourages the LU SA to refer to the expected number and size of the code members.
28. The Board notes that section 4.6 should include a reference to regular reporting, in line with paragraph 72 of the Guidelines, and encourages the LU SA to do so.

### 2.2.6 TRANSPARENT COMPLAINT HANDLING

29. With regard to section 5, the Board recommends the LU SA to include the obligation of the monitoring body to inform the code member, the code owner, the LU SA and where, required, all concerned SAs about the measures taken and its justification without undue delay, in line with paragraph 77 of the Guidelines.
30. Finally, regarding the provision of evidence of suitable corrective measures (section 5.3), the Board encourages the LU SA to amend the text, in order to establish the obligation of the monitoring body to provide evidence of suitable and, if necessary, immediate corrective measures.

### 2.2.7 COMMUNICATION WITH THE LU SA

31. The Board notes that section 6.2 refers to changes “to the basis of accreditation”. Based on the explanations provided by the LU SA, the Board understands that it refers to changes having an impact on the compliance to the accreditation requirements. The Board encourages the LU SA to add such clarification.

### 2.2.8 REVIEW MECHANISMS

32. As stated in the LU SA’s draft accreditation requirements (section 7.2), the monitoring body shall ensure that it has documented plans and procedures to review the operation of the code to ensure that the code remains relevant to the members. In this respect, the Board underlines that changes in the application and interpretation of the law and new technological developments should be taken into consideration. Therefore, the Board encourages the LU SA to reflect it in the text.
33. The Board notes that under section 7.2 of the requirements there is no reference to the fact that the updating of the code of conduct is the responsibility of the code owner. The Board is of the opinion that, in order to avoid confusion, a reference to the code owner should be made. Therefore, the Board encourages the LU SA to add that the monitoring body shall apply and implement updates, amendments, and/or extensions to the Code, as decided by the code owner.
34. In addition, the Board considers that the annual report on the operation of the code should be at the disposal of the LU SA, and encourages the LU SA to amend the draft accordingly.

### 2.2.9 LEGAL STATUS

35. The Board encourages the LU SA to replace the term “European Union” by “European Economic Area” in section 8.1.
36. Regarding section 9, the EDPB recommends the LU SA to add that, when subcontractors are used, the monitoring body shall ensure effective monitoring of the services provided by the contracting entities. Moreover, the Board underlines the need to specify requirements relating to the termination of the contract, in particular so as to ensure that the subcontractors fulfil their data protection obligations,

and encourages the LU SA to add such remark. Finally, the Board encourages the LU SA to provide examples of when subcontracting is allowed and to delete the sentence related to subcontracting in “punctual circumstances”.

### 3 CONCLUSIONS / RECOMMENDATIONS

37. The draft accreditation requirements of the Luxembourgish Supervisory Authority may lead to an inconsistent application of the accreditation of monitoring bodies and the following changes need to be made:
38. Regarding *general remarks* the Board recommends that the LU SA:
  1. to add a reference to the Guidelines 04/2021, which are relevant in the context of monitoring codes of conduct intended for international transfers.
  2. make explicit that an internal monitoring body cannot be setup within a code member.
  3. formulate the requirements as an obligation.
39. Regarding *independence* the Board recommends that the LU SA:
  1. include a reference to a separate accountability
  2. add a requirement to prove that the internal monitoring body has a specific separated budget that is able to manage independently
40. Regarding *conflict of interest* the Board recommends that the LU SA:
  1. align the text with the Guidelines and include the obligation of the monitoring body to refrain from any action that is incompatible with its tasks and duties
41. Regarding *expertise* the Board recommends that the LU SA:
  1. clarify the differences between the three types of personnel and ensure consistency in the requirements, in order to not curtail the freedom of the code owner to define the type of expertise required for each role.
42. Regarding *transparent complaint handling* the Board recommends that the LU SA:
  1. include the obligation of the monitoring body to inform the code member, the code owner, the LU SA and where, required, all concerned SAs about the measures taken and its justification without undue delay, in line with paragraph 77 of the Guidelines.
43. Regarding *legal status* the Board recommends that the LU SA:
  1. add in section 9 that, when subcontractors are used, the monitoring body shall ensure effective monitoring of the services provided by the contracting entities

## 4 FINAL REMARKS

44. This opinion is addressed to the Luxembourgish supervisory authority and will be made public pursuant to Article 64 (5) (b) GDPR.
45. According to Article 64 (7) and (8) GDPR, the LU SA shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft decision. Within the same period, it shall provide the amended draft decision or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.
46. The LU SA shall communicate the final decision to the Board for inclusion in the register of decisions, which have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Adopted

# Opinion of the Board (Art. 64)



**Opinion 16/2022 on the draft decision of the competent supervisory authority of Slovenia regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR**

**Adopted on 4 July 2022**

## Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT .....	4
2.1	General reasoning of the Board regarding the submitted draft accreditation requirements.....	4
2.2	Analysis of the SI SA's accreditation requirements for Code of Conduct's monitoring bodies ....	5
2.2.1	GENERAL REMARKS .....	5
2.2.2	INDEPENDENCE .....	6
2.2.3	CONFLICT OF INTEREST.....	7
2.2.4	EXPERTISE .....	7
2.2.5	ESTABLISHED PROCEDURES AND STRUCTURES.....	7
2.2.6	TRANSPARENT COMPLAINT HANDLING .....	7
2.2.7	COMMUNICATION WITH THE SI SA.....	8
2.2.8	REVIEW MECHANISMS .....	8
2.2.9	SUBCONTRACTORS.....	8
3	CONCLUSIONS / RECOMMENDATIONS .....	8
4	FINAL REMARKS.....	9

## **The European Data Protection Board**

Having regard to Article 63, Article 64 (1)(c), (3)-(8) and Article 41 (3) 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 10 and Article 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the European Data Protection Board (hereinafter “the Board”) is to ensure the consistent application of the GDPR when a supervisory authority (hereinafter “SA”) intends to approve the requirements for accreditation of a code of conduct (hereinafter “code”) monitoring body pursuant to article 41. The aim of this opinion is therefore to contribute to a harmonised approach with regard to the suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a code monitoring body by the competent supervisory authority. Even though the GDPR does not directly impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinion by: firstly, requesting the competent SAs to draft their requirements for accreditation of monitoring bodies based on article 41(2) GDPR and on the Board’s “Guidelines 1/2019 on Codes of Conduct and Monitoring bodies under Regulation 2016/679” (hereinafter the “Guidelines”), using the eight requirements as outlined in the guidelines’ accreditation section (section 12); secondly, providing the competent SAs with written guidance explaining the accreditation requirements; and, finally, requesting the competent SAs to adopt the requirements in line with this opinion, so as to achieve an harmonised approach.

(2) With reference to article 41 GDPR, the competent supervisory authorities shall adopt requirements for accreditation of monitoring bodies of approved codes. They shall, however, apply the consistency mechanism in order to allow the setting of suitable requirements ensuring that monitoring bodies carry out the monitoring of compliance with codes in a competent, consistent and independent manner, thereby facilitating the proper implementation of codes across the Union and, as a result, contributing to the proper application of the GDPR.

(3) In order for a code covering non-public authorities and bodies to be approved, a monitoring body (or bodies) must be identified as part of the code and accredited by the competent SA as being capable of effectively monitoring the code. The GDPR does not define the term “accreditation”. However, article 41 (2) of the GDPR outlines general requirements for the accreditation of the monitoring body. There are a number of requirements, which should be met in order to satisfy the competent supervisory authority to accredit a monitoring body. Code owners are required to explain and demonstrate how their proposed monitoring body meets the requirements set out in article 41 (2) GDPR to obtain accreditation.

---

<sup>1</sup> References to the “Union” made throughout this opinion should be understood as references to “EEA”.

(4) While the requirements for accreditation of monitoring bodies are subject to the consistency mechanism, the development of the accreditation requirements foreseen in the Guidelines should take into consideration the code's sector or specificities. Competent supervisory authorities have discretion with regard to the scope and specificities of each code, and should take into account their relevant legislation. The aim of the Board's opinion is therefore to avoid significant inconsistencies that may affect the performance of monitoring bodies and consequently the reputation of GDPR codes of conduct and their monitoring bodies.

(5) In this respect, the Guidelines adopted by the Board will serve as a guiding thread in the context of the consistency mechanism. Notably, in the Guidelines, the Board has clarified that even though the accreditation of a monitoring body applies only for a specific code, a monitoring body may be accredited for more than one code, provided it satisfies the requirements for accreditation for each code.

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

#### **HAS ADOPTED THE FOLLOWING OPINION:**

## **1 SUMMARY OF THE FACTS**

1. The Slovenian Supervisory Authority (hereinafter "SI SA") has submitted its draft decision containing the accreditation requirements for a code of conduct monitoring body to the Board, requesting its opinion pursuant to article 64 (1)(c), for a consistent approach at Union level. The decision on the completeness of the file was taken on 28 March 2022.

## **2 ASSESSMENT**

### **2.1 General reasoning of the Board regarding the submitted draft accreditation requirements**

2. All accreditation requirements submitted to the Board for an opinion must fully address article 41 (2) GDPR criteria and should be in line with the eight areas outlined by the Board in the accreditation section of the Guidelines (section 12, pages 21-25). The Board opinion aims at ensuring consistency and a correct application of article 41 (2) GDPR as regards the presented draft.
3. This means that, when drafting the requirements for the accreditation of a body for monitoring codes according to articles 41 (3) and 57 (1) (p) GDPR, all the SAs should cover these basic core requirements foreseen in the Guidelines, and the Board may recommend that the SAs amend their drafts accordingly to ensure consistency.
4. All codes covering non-public authorities and bodies are required to have accredited monitoring bodies. The GDPR expressly request SAs, the Board and the Commission to "encourage the drawing up of codes of conduct intended to contribute to the proper application of the GDPR, taking account of the specific

features of the various processing sectors and the specific needs of micro, small and medium sized enterprises.” (Article 40 (1) GDPR). Therefore, the Board recognises that the requirements need to work for different types of codes, applying to sectors of diverse size, addressing various interests at stake and covering processing activities with different levels of risk.

5. In some areas, the Board will support the development of harmonised requirements by encouraging the SI SA to consider the examples provided for clarification purposes.
6. When this opinion remains silent on a specific requirement, it means that the Board is not asking the SI SA to take further action.
7. This opinion does not reflect upon items submitted by the SI SA, which are outside the scope of article 41 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

## 2.2 Analysis of the SI SA’s accreditation requirements for Code of Conduct’s monitoring bodies

8. Taking into account that:
  - a. Article 41 (2) GDPR provides a list of accreditation areas that a monitoring body need to address in order to be accredited;
  - b. Article 41 (4) GDPR requires that all codes (excluding those covering public authorities per Article 41 (6)) have an accredited monitoring body; and
  - c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for monitoring bodies and conduct the accreditation of a body for monitoring codes of conduct.

the Board is of the opinion that:

### 2.2.1 GENERAL REMARKS

9. The Board notes that on 22 February 2022, “the Guidelines 04/2021 on Codes of Conduct as tools for transfers” were adopted. These guidelines do not add any additional requirements for the accreditation of monitoring bodies that monitor codes of conduct intended for international transfers. Rather, the guidelines provide further specifications of the general requirements established by the Guidelines 1/2019 (Section 12) taking into account the specific context of international transfers<sup>2</sup>. For the sake of clarity, the Board recommends the SI SA to add a reference to the above-mentioned guidelines, which are relevant in the context of monitoring codes of conduct intended for international transfers.
10. For the sake of consistency, the Board encourages the SI SA to adjust the terminology used in the requirements to the one used in the Guidelines, this applies in particular to the following terms. This applies in particular to sections 1.2.1 and 4.2, where it should be referred to the “expected number and size of the code members, as well as the complexity or degree of risk of the relevant data processing”. In addition, section 4.2 should refer to the need for monitoring bodies to “actively and effectively monitor compliance”, as well as the need for review procedures to include “specific incidents”. Moreover, section

---

<sup>2</sup> See Section4.2 of the EDPB Guidelines 04/2021 on Codes of Conduct as tools for transfers

4.3 should refer to “annual inspections” and “regular reporting”. Finally, the term “corrective measures” should be used instead of “measures” in sections 4.5 and 5.5.

11. Moreover, the Board is of the opinion that internal monitoring bodies cannot be set up within a code member, but only within a code owner. Therefore, the Board recommends that this is clarified and reflected in the text of the draft accreditation requirements. In addition, the Board encourages the SI SA to include either in the draft accreditation requirements or in the complementary guidance to the requirements examples of what may constitute an internal monitoring bodies (i.e. ad hoc internal committee or separate department within the organisation of the code owner).

## 2.2.2 INDEPENDENCE

12. With respect to the definition of independence, the Board encourages the SI SA to elaborate what independence means. To ensure consistency, such clarification could rely on the wording agreed by the Board in the previous opinions, by specifying that the rules and procedures shall allow the monitoring body to perform the monitoring of compliance with a code of conduct in complete autonomy, without being directly or indirectly influenced nor subject to any form of pressure that might affect its decisions.
13. As regards the legal status and decision-making process of the SI SA’s draft accreditation requirements (section 1.1), the Board acknowledges the duty of independence of the monitoring body from the code owner and the “other subjects” to which the code applies. In this regard, the Board encourages the SI SA to clarify which are the “other subjects” that might influence the decisions of the monitoring bodies by referring to “the code members, the profession, industry or sector to which the code applies and the code owner itself” (Paragraph 63 of the Guidelines).
14. With regard to the same section, last sentence, the Board encourages the SI SA to clarify that the requirement to demonstrate the implementation of complementary measures applies to “internal monitoring bodies”, which shall ensure that the independence of their “monitoring activities” is not at stake. Furthermore, the Board encourages the SI SA to amend this section to reflect the requirement, as provided in paragraph 65 of the Guidelines, that the internal monitoring body has separate staff and management from other areas of the organisation.
15. Moreover, as the section 1.1.4 refers to the terms “undue” influence, the Board encourages the SI SA to delete the word “undue” considering that a monitoring body must be free not only from “undue” but from any external influence.
16. Further, in section 1.2.2, a reference not only to financial resources but also to other resources should be mentioned. Therefore, the Board recommends that the SI SA require that the monitoring body should have access to adequate financial and “other resources” to fulfil its monitoring responsibilities.
17. Finally, with respect to internal monitoring bodies (section 1.2.4), the Board recommends the SI SA to add a requirement to prove that the internal monitoring body has a specific separated budget that is able to manage independently.
18. With regard to section 1.3 of the draft requirements, the Board observes that the reference to organisational independence of the monitoring body is not entirely complete. In particular, the Board notes that the monitoring bodies should be composed of an adequate number of personnel so that they are able to fully carry out the monitoring functions, reflecting the sector concerned and the risks of the processing activities addressed by the code of conduct. Personnel of the monitoring body shall be responsible and shall retain authority for their decisions regarding the monitoring activities. These organisational aspects could be demonstrated not only through the procedure to appoint the monitoring

body personnel, the remuneration of the said personnel, the duration of the personnel's mandate, but also through contract or other formal agreement with the monitoring body. Therefore, the Board recommends that the SI SA provide the above-mentioned references regarding the independence of the monitoring body in performing its tasks and exercising its powers, in accordance with the Guidelines.

19. In addition, the Board encourages the SI SA to, in line with what is mentioned under paragraph 14 of this Opinion, amend the requirement in section 1.3.4 in order to reflect the need for internal monitoring bodies to have separate staff and management.

#### **2.2.3 CONFLICT OF INTEREST**

20. As a general remark in this section, the Board is of the opinion that, for practical reasons, more detailed guidance as to in which situations a conflict of interest could arise might be helpful. An example of a conflict of interest situation would be the case where personnel conducting audits or making decisions on behalf of a monitoring body had previously worked for the code owner, or for any of the organisations adhering to the code. Therefore, the Board encourages the SI SA to add some guidance, similar to the one provided in this paragraph.
21. Moreover, the Board encourages the SI SA to clarify in section 2.3 that the staff chosen by the monitoring body or other body should be "independent of the code member".

#### **2.2.4 EXPERTISE**

22. With regard to section 3.1, the Board acknowledges the requirement for the monitoring body to demonstrate that it has expertise in relation to the specific data processing activities addressed by the code. However, as agreed by the Board in the previous opinions, other factors such as the size of the sector concerned, the different interests involved and the risks of these processing activities should be taken into account. The Board therefore recommends that this is clarified in the draft accreditation requirements.
23. Moreover, the Board notes that SI SA's expertise requirements do not differentiate between staff at the management level and, therefore, in charge of the decision-making process, and staff at the operating level, conducting the monitoring activities. In this regard, the Board encourages the SI SA to clarify in section 3.2 which requirement should be met by the staff performing the monitoring function and the personnel making the decisions.

#### **2.2.5 ESTABLISHED PROCEDURES AND STRUCTURES**

24. Regarding section 4.1, the Board notes that when new members join the code, the monitoring body should, in any case, have a procedure in place to verify that the processing of personal data by these members falls within the scope of the code in question. Therefore, the Board encourages the SI SA not to formulate this provision as an example.

#### **2.2.6 TRANSPARENT COMPLAINT HANDLING**

25. The Board observes that section 5.5 of the SI SA's draft accreditation refers to the obligation of the monitoring body to inform the SA of the measures taken and the reasons for taking them. In line with paragraph 77 of the Guidelines, the Board recommends that the SI SA clarify that this communication should be made "without undue delay", and provide that this notification should be made to "the code member, the code owner, the competent SA and, where required, all concerned SAs".
26. Regarding section 5.8 of the SI SA's draft accreditation requirements, the Board notes that the monitoring body shall, on a regular basis, publish statistical data with the results of the monitoring activities. Without

prejudice to national legislation, the Board encourages the SI SA to amend this requirement so that decisions are published when they relate to repeated and/or serious violations, such as the ones that could lead to the suspension or exclusion of the controller or processor concerned from the code, otherwise publication of summaries of decisions or statistical data should be considered adequate.

#### 2.2.7 COMMUNICATION WITH THE SI SA

27. The Board understands that section 6.1 of the requirements refers to the information that the monitoring body will provide to the SI SA upon request. The Board is of the opinion that the requirement to communicate “any actions” need to address such areas as: actions taken in cases of infringement of the code and the reasons for taking them (article 41 (4) GDPR), periodic reports, reviews or audit findings. Therefore, the Board encourages the SI SA to clarify this requirement accordingly.
28. In addition, the Board recommends that the SI SA clarify the notion of “substantial changes” in section 6.2. In particular, it should be specified that substantial changes include but are not limited to any changes that impacts the ability of the monitoring body to perform its tasks in an independent, impartial and efficient manner. In addition, it should be clarified that not only the above-mentioned changes but also the one listed in section 6.3 are to be communicated to the SI SA without undue delay. Finally, the Board encourages the SI SA to clarify in its draft accreditation requirements the notion of “any changes to the basis of accreditation” referred to in subsection 6.3, point c.

#### 2.2.8 REVIEW MECHANISMS

29. The draft accreditation requirements (section 7.1, second sentence) refer to the possibility for any other entity referred to in the code to be granted an active and participative role in the code review process. The Board notes it is the role of the code owner to ensure the continued relevance and compliance of the code of conduct with applicable legislation. Whilst the monitoring body is not responsible to carry out that task, it shall contribute to any review of the code. The Board therefore encourages the SI SA to specify that the monitoring body shall apply and implement these updates, amendments, and/or extensions to the Code on behalf of the code owner.
30. In addition, the Board encourages the SI SA to specify in section 7.4 that the annual report prepared by the monitoring body should include reviews and/or changes made to the code.

#### 2.2.9 SUBCONTRACTORS

31. In relation to section 9.3, the Board encourages the SI SA to better clarify that notwithstanding the subcontractor’s responsibility and obligations, the monitoring body is always the ultimate responsible for the decision-making and for compliance.
32. Furthermore, the Board recommends that the SI SA clarify the notion of “substantial changes” in section 9.2., in line with what is mentioned under paragraph 28 of this Opinion.

### 3 CONCLUSIONS / RECOMMENDATIONS

9. The draft accreditation requirements of the Slovenian Supervisory Authority may lead to an inconsistent application of the accreditation of monitoring bodies and the following changes need to be made:
10. Regarding *general remarks* the Board recommends that the SI SA:

- to add a reference to the Guidelines 04/2021, which are relevant in the context of monitoring codes of conduct intended for international transfers.
- clarify in the text of the requirements that internal monitoring bodies cannot be set up within a code member, but only within a code owner.

11. Regarding *independence* the Board recommends that the SI SA:

- provide in section 1.1.4 the requirement for monitoring bodies to have access to adequate financial and “other resources” to fulfil their monitoring responsibilities.
- add in section 1.2.4 a requirement to prove that the internal monitoring body has a specific separated budget that is able to manage independently.
- include in section 1.3 the references mentioned in paragraph 18 of this Opinion concerning the independence of the monitoring body in performing its tasks and exercising its powers.

12. Regarding *expertise* the Board recommends that the SI SA:

- clarify that other factors such as the size of the sector concerned, the different interests involved and the risks of these processing activities should be taken into account in order to assess the level of expertise of the monitoring body.

13. Regarding *transparent complaint handling* the Board recommends that the SI SA:

- clarify that the obligation of the monitoring body to communicate the measures taken and the reasons for taking them should take place “without undue delay”, and provide that this notification should be made not only to the SA but also to “the code member, the code owner, the competent SA and all concerned SAs”.

14. Regarding *communication with the SI SA* the Board recommends that the SI SA:

- clarify in section 6.2 that substantial changes include but are not limited to any changes that impacts the ability of the monitoring body to perform its tasks in an independent, impartial and efficient manner, and specify that the changes listed in section 6.3 are to be communicated to the SI SA without undue delay.

15. Regarding *legal status* the Board recommends that the SI SA:

- clarify the notion of “substantial changes” in section 9.2 in line with what is mentioned under paragraph 28 of this Opinion.

## 4 FINAL REMARKS

- This opinion is addressed to the Slovenian supervisory authority and will be made public pursuant to Article 64 (5) (b) GDPR.
- According to Article 64 (7) and (8) GDPR, the SI SA shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft decision. Within the same period, it shall provide the amended draft decision or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

18. The SI SA shall communicate the final decision to the Board for inclusion in the register of decisions, which have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

# Opinion of the Board (Art. 64)



**Opinion 17/2022 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of the ANTOLIN Group**

**Adopted on 1 August 2022**

## Table of contents

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT.....	5
3	CONCLUSIONS / RECOMMENDATIONS.....	5
4	FINAL REMARKS.....	6

## The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 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 European Economic Area (hereinafter “**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 the judgment of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings is intended to provide guarantees that apply uniformly in all third countries and, consequently, independently of the level of protection guaranteed in each third country. The specific requirements

---

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

listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party<sup>2</sup>, endorsed by the EDPB.

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB<sup>3</sup>. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU .

(6) The WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for controllers (hereinafter “**BCR-C**”), including the Intra-Company Agreement where applicable, and the application form. The WP264 of the Article 29 Working Party<sup>4</sup>, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev.01. Additionally, the WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs’ national laws. The EDPB is subject to Regulation 1049/2001<sup>5</sup> pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data<sup>6</sup>.

---

<sup>2</sup> The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

<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, WP 256 rev.01.

<sup>4</sup> Article 29 Working Party, Recommendations on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP264.

<sup>5</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.

<sup>6</sup> This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

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

**HAS ADOPTED THE FOLLOWING OPINION:**

## 1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of the Grupo Antolín Irausa, S.A. and its subsidiaries (hereinafter “**ANTOLIN Group**”) was reviewed by the Spanish SA as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-C of the ANTOLIN Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 7 June 2022. The decision on the completeness of the file was taken on 4 July 2022.

## 2 ASSESSMENT

3. The draft BCR-C of the ANTOLIN Group covers personal data processed by Grupo Antolin Irausa S.A. or any of its subsidiaries that are transferred, directly or indirectly, to subsidiaries outside the EEA. Personal data processing within the EEA is covered by the Privacy Policy of the ANTOLIN Group<sup>7</sup>.
4. Concerned data subjects include suppliers’ representatives, clients’ representatives, employees, employees’ relatives and candidates<sup>8</sup>.
5. The draft BCR-C of the ANTOLIN Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-C of the ANTOLIN Group contains all the elements required under Article 47 GDPR and WP256 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

## 3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the *Intragroup Agreement regarding Binding Corporate Rules*, the EDPB considers that the draft decision of the BCR Lead may be adopted as it is, since the draft BCR-C of the ANTOLIN Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries

---

<sup>7</sup> Section 3.1 of the BCR-C.

<sup>8</sup> Section 3.2 of the BCR-C.

included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.

7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

## 4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

# Opinion of the Board (Art. 64)



**Opinion 02/2023 on the draft decision of the competent supervisory authority of Latvia regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Article 41 GDPR**

**Adopted on 3 February 2023**

## Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT .....	4
2.1	General reasoning of the Board regarding the submitted draft accreditation requirements.	4
2.2	Analysis of the LV SA's accreditation requirements for Code of Conduct's monitoring bodies	
	5	
2.2.1	GENERAL REMARKS .....	5
2.2.2	INDEPENDENCE .....	6
2.2.3	CONFLICT OF INTEREST.....	8
2.2.4	EXPERTISE .....	9
2.2.5	ESTABLISHED PROCEDURES AND STRUCTURES .....	9
2.2.6	TRANSPARENT COMPLAINT HANDLING.....	10
2.2.7	COMMUNICATION WITH THE LV SA .....	10
2.2.8	REVIEW MECHANISMS.....	11
2.2.9	LEGAL STATUS.....	11
3	CONCLUSIONS / RECOMMENDATIONS .....	11
4	FINAL REMARKS.....	13

## **The European Data Protection Board**

Having regard to Article 63, Article 64 (1)(c), (3)-(8) and Article 41 (3) 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 10 and Article 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the European Data Protection Board (hereinafter “the Board”) is to ensure the consistent application of the GDPR when a supervisory authority (hereinafter “SA”) intends to approve the requirements for accreditation of a code of conduct (hereinafter “code”) monitoring body pursuant to Article 41. The aim of this opinion is therefore to contribute to a harmonised approach with regard to the suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a code monitoring body by the competent supervisory authority. Even though the GDPR does not directly impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinion by: firstly, requesting the competent SAs to draft their requirements for accreditation of monitoring bodies based on article 41(2) GDPR and on the Board’s “Guidelines 1/2019 on Codes of Conduct and Monitoring bodies under Regulation 2016/679” (hereinafter the “Guidelines”), using the eight requirements as outlined in the guidelines’ accreditation section (section 12); secondly, providing the competent SAs with written guidance explaining the accreditation requirements; and, finally, requesting the competent SAs to adopt the requirements in line with this opinion, so as to achieve a harmonised approach.

(2) With reference to Article 41 GDPR, the competent supervisory authorities shall adopt requirements for accreditation of monitoring bodies of approved codes. They shall, however, apply the consistency mechanism in order to allow the setting of suitable requirements ensuring that monitoring bodies carry out the monitoring of compliance with codes in a competent, consistent and independent manner, thereby facilitating the proper implementation of codes across the Union and, as a result, contributing to the proper application of the GDPR.

(3) In order for a code covering non-public authorities and bodies to be approved, a monitoring body (or bodies) must be identified as part of the code and accredited by the competent SA as being capable of effectively monitoring the code. The GDPR does not define the term “accreditation”. However, Article 41 (2) of the GDPR outlines general requirements for the accreditation of the monitoring body. There are a number of requirements, which should be met in order to satisfy the competent supervisory authority to accredit a monitoring body. Code owners are required to explain and

---

<sup>1</sup> References to the “Union” made throughout this opinion should be understood as references to “EEA”.

demonstrate how their proposed monitoring body meets the requirements set out in Article 41 (2) GDPR to obtain accreditation.

(4) While the requirements for accreditation of monitoring bodies are subject to the consistency mechanism, the development of the accreditation requirements foreseen in the Guidelines should take into consideration the code's sector or specificities. Competent supervisory authorities have discretion with regard to the scope and specificities of each code, and should take into account their relevant legislation. The aim of the Board's opinion is therefore to avoid significant inconsistencies that may affect the performance of monitoring bodies and consequently the reputation of GDPR codes of conduct and their monitoring bodies.

(5) In this respect, the Guidelines adopted by the Board will serve as a guiding thread in the context of the consistency mechanism. Notably, in the Guidelines, the Board has clarified that even though the accreditation of a monitoring body applies only for a specific code, a monitoring body may be accredited for more than one code, provided it satisfies the requirements for accreditation for each code.

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

#### **HAS ADOPTED THE FOLLOWING OPINION:**

## **1 SUMMARY OF THE FACTS**

1. The Latvian supervisory authority (hereinafter "LV SA") has submitted its draft decision containing the accreditation requirements for a code of conduct monitoring body to the Board, requesting its opinion pursuant to Art. 64 (1)(c), for a consistent approach at Union level. The decision on the completeness of the file was taken on 28 October 2022.
2. In compliance with article 10 (2) of the Board Rules of Procedure, due to the complexity of the matter at hand, the Chair decided to extend the initial adoption period of eight weeks by a further six weeks.

## **2 ASSESSMENT**

### **2.1 General reasoning of the Board regarding the submitted draft accreditation requirements**

3. All accreditation requirements submitted to the Board for an opinion must fully address Art. 41 (2) GDPR criteria and should be in line with the eight areas outlined by the Board in the accreditation section of the Guidelines (section 12, pages 21-25). The Board opinion aims at ensuring consistency and a correct application of Art. 41 (2) GDPR as regards the presented draft.
4. This means that, when drafting the requirements for the accreditation of a body for monitoring codes according to Art. 41 (3) and 57 (1) (p) GDPR, all the SAs should cover these basic core requirements

foreseen in the Guidelines, and the Board may recommend that the SAs amend their drafts accordingly to ensure consistency.

5. All codes covering non-public authorities and bodies are required to have accredited monitoring bodies. Art. 40 GDPR expressly request SAs, the Board and the Commission to “encourage the drawing up of codes of conduct intended to contribute to the proper application of the GDPR, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium sized enterprises.” Therefore, the Board recognises that the requirements need to work for different types of codes, applying to sectors of diverse size, addressing various interests at stake and covering processing activities with different levels of risk.
6. In some areas, the Board will support the development of harmonised requirements by encouraging the SA to consider the examples provided for clarification purposes.
7. When this opinion remains silent on a specific requirement, it means that the Board is not asking the LV SA to take further action.
8. This opinion does not reflect upon items submitted by the LV SA, which are outside the scope of Art. 41 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

## 2.2 Analysis of the LV SA’s accreditation requirements for Code of Conduct’s monitoring bodies

9. Taking into account that:
  - a. Art. 41 (2) GDPR provides a list of accreditation areas that a monitoring body need to address in order to be accredited;
  - b. Art. 41 (4) GDPR requires that all codes (excluding those covering public authorities per Art. 41 (6)) have an accredited monitoring body; and
  - c. Art. 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for monitoring bodies and conduct the accreditation of a body for monitoring codes of conduct.

the Board is of the opinion that:

### 2.2.1 GENERAL REMARKS

10. The Board notes that the reference to the processing carried out by public authorities and bodies provided under section 15 of the Guidelines is missing and, therefore, the Board recommend the LV SA to include such a reference.
11. For the sake of consistency and clarity, the Board encourages the LV SA to replace throughout the draft accreditation requirements the term “LVSA” with the term “Competent Supervisory Authority” in line with the terminology used in the Guidelines. At the same time the Board encourages the LV SA to introduce in the draft requirements a definition of the term “Competent Supervisory Authority”, to be understood as the Data State Inspectorate of the Republic of Latvia.

12. For the sake of consistency, the Board encourages the LV SA to adjust terminology used in the requirements to the terminology used in the Guidelines, this applies to the terms ‘code owners’, i. e. to include “and in line with national law”.
13. In general, the Board encourages the LV SA to ensure consistency of the wording throughout the text. For instance, in section 4.1 the term “appropriate” expertise is used, while in section 4.3 the word “adequate” experience and knowledge is introduced.
14. The Board encourages the LV SA, for the sake of consistency, to use the word/wording “influence” instead of “pressure” (section 2.1.1.e), “mitigate” instead of “make appropriate provisions for” (section 2.1.2.g), “previous and planned” or “previous, current and upcoming” instead of “past or projected” (section 2.2.7.a), “influence” instead of “interference” (section 2.3.1.e, section 3.1.b), “carry out” instead of “discharge”(section 4.1, section 4.3), “shall introduce” instead of “has introduced” (section 5.2), “understandable” instead of “understood” (section 6.1.a).
15. The Board notes that on 22 February 2022, “the Guidelines 04/2021 on Codes of Conduct as tools for transfers” were adopted. These guidelines do not add any additional requirements for the accreditation of monitoring bodies that monitor codes of conduct intended for international transfers. Rather, the guidelines provide further specifications of the general requirements established by the Guidelines (Section 12), taking into account the specific context of international transfers.<sup>2</sup> For the sake of clarity, the Board recommends the LV SA to add a reference to the above-mentioned guidelines, which are relevant in the context of monitoring codes of conduct intended for international transfers.
16. With reference to section 1.3, the Board understands that when referring to transnational application, a translation into Latvian of the documents submitted in another language shall be attached. Therefore, the Board encourages the LV SA to clarify if the understanding of the Board is correct.
17. The Board notes that letters a and b 4 under section 1.6 of the LV SA’s draft accreditation requirements would be better placed in section 3 as evidence in regard to requirements relating to the absence of conflict of interest. Thus, in order to avoid confusion, the EDPB encourages the LV SA to move the paragraphs accordingly.

## 2.2.2 INDEPENDENCE

18. With regard to section 2.1 (“Legal status and organisational independence”), for the sake of clarity the Board encourages the LV SA to redraft this section by stating that the monitoring body can act as an internal or external monitoring body vis-à-vis the code owner, “with the choice of a particular approach at the discretion of the code owner”.
19. With regard to section 2.1.b, the Board recommends the LV SA to add the wording “appropriately independent in relation to its impartiality of function”, as provided by paragraph 63 of the Guidelines.
20. With regard to section 2.1.1.c, the Board recommends the LV SA to add the following word “full” when it refers to autonomy, as provided by paragraph 67 of Guidelines.
21. With regard to section 2.1.1.f, in order to provide the same understanding as the one in paragraph 67 of Guidelines, the Board encourages the LV SA to add a reference referring to the independence “in performing its tasks and exercising its power”.

---

<sup>2</sup> See Section4.2 of the EDPB Guidelines 04/2021 on Codes of Conduct as tools for transfers.

22. With regard to section 2.1.2.a, the Board understands that the appointment refers to "members/staff". However, in order to avoid confusion, the Board encourages the LV SA to make it clearer.
23. With regard to section 2.1.2.d, the Board encourages the LV SA to clarify that the declaration shows there are no common interests with the entities to be monitored.
24. With regard to section 2.1.2.g, the Board underlines that, according to paragraph 66 of the Guidelines, the independence of a monitoring body should be demonstrated by appropriate safeguards in place to sufficiently mitigate a risk of independence *or a conflict of interest*. Moreover, a monitoring body will need to identify risks to its *impartiality* on an ongoing basis. The LV SA's draft accreditation requirements do not include such references to "conflict of interest" and "impartiality" and, therefore, the Board recommends to amend section 2.1.2.g accordingly.
25. Moreover, with regard to the financial support (section 2.2.3), the Board observes that the draft accreditation requirements refer to the means that "shall not adversely affect its independence". The Board encourages the LV SA to redraft the relevant part of the requirements by adding a reference to "in relation to the task of monitoring compliance with the Code".
26. In addition, the Board considers that the requirements on financial resources would benefit from the inclusion of some examples with regard to the financial independence of the monitoring body, in order to highlight how the monitoring body can demonstrate that the means by which it obtains financial support should not adversely affect its independence (section 2.2). For instance, the monitoring body would not be considered financially independent if the rules governing its financial support allow a code member, who is under investigation by the monitoring body, to stop its financial contributions to it, in order to avoid a potential sanction from the monitoring body. The Board encourages the LV SA to add such clarification and provide examples of how the monitoring body can provide such evidence.
27. With respect to internal monitoring bodies (section 2.2.7), the Board recommends the LV SA to add a requirement to prove that the internal monitoring body has a specific separated budget that the monitoring body is able to manage independently.
28. Finally, monitoring bodies must have sufficient financial and other resources together with the necessary procedures to ensure the functioning of the code of conduct over time to ensure long-term financing, e. g. when one or more funding sources are no longer available. That is why, with respect to section 2.2.7 of the draft requirements, the Board encourages the LV SA to add a clear indication that financial stability and resources need to be accompanied with the necessary procedures to ensure the functioning of the code of conduct over time.
29. With regard to section 2.3.1.a, the Board understands that the reference to "payroll system for its personnel" is an example and encourages the LV SA to clarify the wording, by adding the word "including" before the words "has payroll systems".
30. With respect to section 2.3.1.a and the requirements that an internal body has to demonstrate, the Board notes that the requirements from paragraph 65 of Guidelines referring to the use of effective organizational and information barriers and separate reporting management structures for the association and monitoring body were not included. Therefore, the Board recommends the LV SA to add the missing requirements.
31. With respect to section 2.3.1.c, addressing the need for the monitoring body to prove, among others, that it has "adequate" human resources for the effective performance of its functions under Art. 41

- (1) GDPR, the Board encourages the LV SA to consider making a reference to “adequate numbers of sufficiently qualified personnel”.
32. In addition, the Board notes that the monitoring bodies shall be composed of an adequate and proportionate number of personnel. These organisational aspects could be demonstrated not only through the procedure to appoint the monitoring body personnel, the remuneration of the said personnel, the duration of the personnel’s mandate, but also through contract or other formal agreement with the monitoring body. Therefore, the Board recommends that the LV SA provide the above-mentioned references regarding the independence of the monitoring body in performing its tasks and exercising its powers, in accordance with the Guidelines.
  33. With regard to section 2.3.1.d, The Board encourages the LV SA to include either in the draft accreditation requirements or in the complementary guidance to the requirements, some examples of the evidence or documentation required in order to demonstrate the accountability of the monitoring body.
  34. In section 2.3.4.d, the Board recommends that the LV SA adds a clear indication that the monitoring body shall ensure effective monitoring of the services provided by subcontractors.

### 2.2.3 CONFLICT OF INTEREST

35. As a general remark in this section, the Board is of the opinion that, for practical reasons, more detailed examples of cases where a conflict of interest could arise might be helpful. An example of a conflict of interest situation would be the case where personnel conducting audits or making decisions on behalf of a monitoring body had previously worked for the code owner, or for any of the organisations adhering to the code. Therefore, the Board encourages the LV SA to elaborate on the examples included in the explanatory note.
36. With regard to section 3.1.c, the Board underlines that, according to paragraph 68 of the Guidelines, the monitoring body must remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from any person, organisation or association. The LV SA’s draft accreditation requirements do not include references to the terms “whether direct or indirect” or to the term “association” and, therefore, the Board recommends the LV SA to add such references.
37. As regards section 3.1.e, the Board highlights that, according to paragraph 68 of the Guidelines, the body should have its own staff which are chosen by them or some or some other body independent of the code and it should be subject to the exclusive direction of those bodies only. The LV SA’s draft accreditation requirements do not include reference to “other body independent of the code” and, therefore, the Board recommends the LV SA to align the text with the Guidelines by adding “and that other body independent of the code” after the wording “exclusive direction of the monitoring body”.
38. With reference to section 3.2, the Board underlines that, according to paragraph 68 of the Guidelines, the monitoring body shall put in place safeguards not only in regard to conflict of interest but also to any incompatible occupation. The LV SA’s draft accreditation requirements do not include reference to “and any incompatible occupation” and, therefore, the Board recommends the LV SA to add such reference after the wording “potential conflict of interest”.

#### 2.2.4 EXPERTISE

39. With reference to section 4.1, paragraph 69 of the Guidelines states that the monitoring body has the requisite level of expertise. Therefore, the Board recommends the LV SA to align the text with the Guidelines and require to have a “requisite level” expertise instead of “appropriate” expertise.
40. In respect of section 4.2, the Board encourages the LV SA to add also the reference to the previous experience of acting in a monitoring capacity.
41. With regard to sections 4.2.a, 4.2.b and 4.2.c referring to “in-depth knowledge and experience”, the Board recommends the LV SA to follow the wording from paragraph 69 of the Guidelines by replacing “in-depth understanding and expert knowledge”. The Board also recommends to add “data protection issues” to the section 4.2.a as this requirement, specified in paragraph 69 of the Guidelines, is important part of the expert-knowledge as it ensures that personnel of the monitoring body is able to assess and reflect not only the data protection law but also specific legal and practical issues that might be relevant in regard to each specific case.
42. As regards section 4.2.c, the Board underlines that paragraph 69 of the Guidelines refers to auditing, monitoring or quality assurance activities and, therefore, the Board recommends the LV SA to follow the wording from the Guidelines, i.e. by replacing the word “control” with the ones specified in paragraph 69 of the Guidelines.
43. With reference to section 4.4, the Board acknowledges the requirement for the monitoring body to demonstrate that it has expertise in relation to the specific data processing activities addressed by the code. However, as expressed by the Board in previous opinions, other factors such as the size of the sector concerned, the different interests involved and the risks of these processing activities should be taken into account. The Board therefore recommends that this is clarified in the draft accreditation requirements.
44. Moreover, the Board notes that the LV SA’s expertise requirements do not differentiate between staff at the management level and, therefore, in charge of the decision-making process, and staff at the operating level, conducting the monitoring activities. In this regard, the Board encourages the LV SA to clarify in section 4.4 which requirements should be met by the staff performing the monitoring function and the personnel making the decisions.
45. Furthermore, as regards sections 4.6 and 4.7, the Board considers that the requirements for the personnel are very specific and may curtail the freedom of the code owner to define the specific expertise requirements in the code of conduct. The Board encourages the LV SA to make the requirements less restrictive by including a more general reference that takes into account the different types of codes, such as “a relevant level of experience in accordance with the code itself”.
46. In addition, the Board observes that the LV SA makes a distinction between legal and technical personnel. The Board encourages the LV SA to clarify that the technical requirements of the personnel will depend on whether it is necessary for the code at stake.

#### 2.2.5 ESTABLISHED PROCEDURES AND STRUCTURES

47. The Board observes that the requirements based on paragraph 72 of the Guidelines, referring to the publication of audit reports as well as to the findings of periodic reporting from controllers and

processors within the scope of the code, and paragraph 73 of the Guidelines are missing and, therefore, the Board recommends the LV SA to add the missing requirements.

48. With reference to section 5.1, the Board highlights that paragraph 70 of the Guidelines refers to “appropriate governance structures” and procedures. The LV SA’s draft accreditation requirements do not include reference to “appropriate governance structures” and, therefore, the Board recommends the LV SA to add such reference.
49. With regard to section 5.2.a, the Board underlines that paragraph 71 of the Guidelines refers to “controllers and processors” when it comes to the provisions of the code to be met and, therefore, the Board recommends the LV SA to replace “code members” with “controller and processors”.
50. In respect of section 5.2.b, the Board observes that the LV SA’ draft accreditation requirements do not include reference to “random or unannounced audits, annual inspections, regular reporting and the use of questionnaires” as per paragraph 72 of the Guidelines and, therefore, the Board recommends the LV SA to add such a reference. The Board, taking into consideration paragraph 72 of the Guidelines, also recommends to include “specific incidents and the number of members of the code” to the factors that should be considered in regard to procedures specified in section 5.2.b, and those factors is recommended to be drafted in a non-exhaustive list.

#### 2.2.6 TRANSPARENT COMPLAINT HANDLING

51. Regarding section 6, the Board highlights that section 12.5 of the Guidelines refers to “Transparent complaints handling”. Therefore, the Board recommends the LV SA to align the title of this section in line with the Guidelines.
52. With reference to section 6.1 of the LV SA’s draft accreditation requirements, the Board considers that, according to paragraph 74 of the Guidelines, the monitoring body will need to establish effective procedures and structures which can deal with complaints handling in an impartial and transparent manner. Therefore, the Boards recommends the LV SA that the requirement is redrafted accordingly.
53. With regard to section 6.1.b, paragraph 76 of the Guidelines refers to “immediate” suitable measures and, therefore, the Board recommends the LV SA to adapt the wording accordingly.
54. In addition, regarding the remedial actions and sanctions, the Board recommends the LV SA to amend the text in order to make references to “a formal notice requiring the implementation of specific actions within a specified deadline” and “temporary suspension”.
55. Finally, as regards section 6.1.b, the Board understands that the corrective measures refer to the situation when the controller or processor from the code “acts outside the terms of the code”. However, for clarity reasons, the Board encourages the LV SA to make it clearer.

#### 2.2.7 COMMUNICATION WITH THE LV SA

56. The Board notes that under section 7 of the requirements there is no reference to the fact that the updating of the code of conduct is the responsibility of the code owner. The Board is of the opinion that, in order to avoid confusion, a reference to the code owner should be made. Therefore, the Board encourages the LV SA to add that the monitoring body shall apply and implement updates, amendments, and/or extensions to the Code, as decided by the code owner.

- 57. With respect to section 7.2, the Board notes that the LV SA's draft accreditation requirements do not refer to the "effective communication" of any actions carried out by a monitoring body to the LV SA and, therefore, the Board recommends the LV SA to include such a reference.
- 58. As regards section 7.2.f, the Board encourages the LV SA to specify in its draft accreditation requirements that substantial changes include but are not limited to any changes that impacts the ability of the monitoring body to perform its tasks in an independent, impartial and efficient manner.
- 59. In addition, the Board encourages the LV SA to specify in section 7.2.g that the annual report prepared by the monitoring body should include reviews and/or changes made to the code.

#### **2.2.8 REVIEW MECHANISMS**

- 60. The Board observes that the requirement from paragraph 80 of the Guidelines, which states that the monitoring body shall set out appropriate review mechanisms to ensure that the code remains relevant and continues to contribute to the proper application of the GDPR, was not included. Therefore, the Board recommends the LV SA to add the missing requirement.

#### **2.2.9 LEGAL STATUS**

- 61. The Board notes that the requirement from paragraph 81 of the Guidelines, which states that the monitoring body has the appropriate standing to carry out its role under Art. 41(4) and is capable of being fined as per Art. 83 (4) GDPR, was not included. Therefore, the Board recommends the LV SA to add the missing requirement.

### **3 CONCLUSIONS / RECOMMENDATIONS**

- 62. The draft accreditation requirements of the LV Supervisory Authority may lead to an inconsistent application of the accreditation of monitoring bodies and the following changes need to be made:
- 63. Regarding *general remarks* the Board recommends that the LV SA:
  - 1. includes a reference that the monitoring of approved codes of conduct will not apply to processing carried out by public authorities or bodies;
  - 2. adds a reference to the Guidelines 04/2021, which are relevant in the context of monitoring codes of conduct intended for international transfers.
- 64. Regarding *independence* the Board recommends that the LV SA:
  - 1. adds the following wording "appropriately independent in relation to its impartiality of function" in section 2.1.b;
  - 2. adds the word "full" in section 2.1.1.c when it refers to autonomy;
  - 3. redrafts section 2.1.2.g to include references to "conflict of interest" and "impartiality";
  - 4. adds in section 2.2.7 a requirement to prove that the internal monitoring body has a specific separated budget that monitoring body is able to manage independently;
  - 5. adds in section 2.3.1.a a requirement referring to the use of effective organizational and information barriers and separate reporting management structures for the association and monitoring body;

6. includes in section 2.3.1 the references mentioned in paragraph 31 of this Opinion concerning the independence of the monitoring body in performing its tasks and exercising its powers;
  7. makes explicit that the monitoring body shall ensure effective monitoring of the services provided by subcontractors.
65. Regarding *conflict of interest* the Board recommends that the LV SA:
  1. includes in section 3.1.c references to “whether direct or indirect” and “association”, in line with the Guidelines;
  2. aligns the text of the section 3.1.e with the Guidelines by adding “and that other independent body of the code” after the wording “exclusive direction of the monitoring body”;
  3. aligns the text of section 3.2 with the Guidelines by adding “and any incompatible occupation” after the wording “potential conflict of interest”.
66. Regarding *expertise* the Board recommends that the LV SA:
  1. aligns the text of section 4.1 with the Guidelines by using “requisite level” expertise instead of “appropriate” expertise;
  2. replaces “in-depth knowledge and experience” with “in-depth understanding and expert knowledge” in sections 4.2.a, 4.2.b and 4.2.c and adds the wording “data protection issues” in section 4.2.a;
  3. follows the wording of paragraph 69 from the Guidelines, by replacing the word “control” with “auditing, monitoring or quality assurance activities”;
  4. clarifies that other factors such as the size of the sector concerned, the different interests involved and the risks of these processing activities should be taken into account in order to assess the level of expertise required by the monitoring body.
67. Regarding *established procedures and structures* the Board recommends that the LV SA:
  1. includes in section 5.2 a requirement referring to the publication of audit reports as well as to the findings of periodic reporting from controllers and processors within the scope of the code;
  2. includes requirements based on paragraph 73 of the Guidelines;
  3. aligns the text in section 5.1 with the Guidelines by adding “appropriate governance structures” after the wording “has introduced”;
  4. aligns the text of section 5.2.a with the Guidelines by replacing “code members” with “controller and processors”;
  5. adds in section 5.2.b some examples in the requirements, such as random or unannounced audits, annual inspections, regular reporting and the use of questionnaires. In addition, it should be included the “specific incidents and the number of members of the code” to the factors that should be considered in regard to the procedures specified in section 5.2.b and those factors to be drafted in non-exhaustive list.
68. Regarding *transparent complaint handling* the Board recommends that the LV SA:
  1. aligns the title of section 6 with the Guidelines, which refers to “Transparent” complaints handling;

2. redrafts the requirement in section 6.1 in line with paragraph 74 of the Guidelines, by adding that the monitoring body shall establish effective procedures and structures which can deal with complaints handling in an impartial and transparent manner;
  3. aligns the text of section 6.1.b with paragraph 76 of the Guidelines, by adding the word “immediate” before suitable measures. In addition, regarding the remedial actions and sanctions, it should be included a reference to “a formal notice requiring the implementation of specific actions within a specified deadline” and “temporary” suspension.
69. Regarding *communication with the competent supervisory authority* the Board recommends that the LV SA:
1. redrafts section 7.2 to include the reference to the “effective communication” of any actions carried out by a monitoring body to the LV SA;
  2. redrafts section 7.2 to include reference to the “effective communication” to “other supervisory authorities”, as far as transnational codes are concerned.
70. Regarding *review mechanisms* the Board recommends that the LV SA:
1. adds in section 8.1 a requirement stating that the monitoring body shall set out appropriate review mechanisms to ensure that the code remains relevant and continues to contribute to the proper application of the GDPR.
71. Regarding *legal status* the Board recommends that the LV SA:
1. modify section 9.1 in order to include that the monitoring body has the appropriate standing to carry out its role under Article 41(4) and is capable of being fined as per Art. 83(4) GDPR.

## 4 FINAL REMARKS

72. This opinion is addressed to the Latvian supervisory authority and will be made public pursuant to Art. 64 (5) (b) GDPR.
73. According to Art. 64 (7) and (8) GDPR, the LV SA shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft decision. Within the same period, it shall provide the amended draft decision or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.
74. The LV SA shall communicate the final decision to the Board for inclusion in the register of decisions, which have been subject to the consistency mechanism, in accordance with Art. 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

# Opinion of the Board (Art. 64)



**Opinion 1/2023 on the draft decision of the competent supervisory authority of Croatia regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Article 41 GDPR**

Adopted on 3 February 2023

## Table of contents

1	Summary of the Facts.....	4
2	Assessment .....	4
2.1	General reasoning of the EDPB regarding the submitted draft decision.....	4
2.2	Analysis of the HR SA's accreditation requirements for Code of Conduct's monitoring bodies 5	
2.2.1	GENERAL REMARKS.....	5
2.2.2	APPLICATION REQUIREMENTS .....	6
2.2.3	INDEPENDENCE .....	7
2.2.4	CONFLICT OF INTEREST .....	9
2.2.5	EXPERTISE.....	9
2.2.6	ESTABLISHED PROCEDURES AND STRUCTURES.....	9
2.2.7	TRANSPARENT COMPLAINT HANDLING .....	10
2.2.8	COMMUNICATION WITH THE HR SA.....	10
2.2.9	CODE REVIEW MECHANISM .....	11
2.2.10	LEGAL STATUS .....	11
3	Conclusions / Recommendations .....	11
4	Final Remarks .....	13

## The European Data Protection Board

Having regard to Article 63, Article 64 (1)(c), (3)-(8) and Article 41 (3) 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 10 and Article 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the European Data Protection Board (hereinafter “the Board”) is to ensure the consistent application of the GDPR when a supervisory authority (hereinafter “SA”) intends to approve the requirements for accreditation of a code of conduct (hereinafter “code”) monitoring body pursuant to Article 41 GDPR. The aim of this opinion is therefore to contribute to a harmonised approach with regard to the suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a code monitoring body by the competent supervisory authority. Even though the GDPR does not directly impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinion by: firstly, requesting the competent SAs to draft their requirements for accreditation of monitoring bodies based on Article 41 (2) GDPR and on the Board’s “Guidelines 1/2019 on Codes of Conduct and Monitoring bodies under Regulation 2016/679” (hereinafter the “Guidelines”), using the eight requirements as outlined in the guidelines’ accreditation section (section 12); secondly, providing the competent SAs with written guidance explaining the accreditation requirements; and, finally, requesting the competent SAs to adopt the requirements in line with this opinion, so as to achieve an harmonised approach.

(2) With reference to Article 41 GDPR, the competent supervisory authorities shall adopt requirements for accreditation of monitoring bodies of approved codes. They shall, however, apply the consistency mechanism in order to allow the setting of suitable requirements ensuring that monitoring bodies carry out the monitoring of compliance with codes in a competent, consistent and independent manner, thereby facilitating the proper implementation of codes across the Union and, as a result, contributing to the proper application of the GDPR.

(3) In order for a code covering non-public authorities and bodies to be approved, a monitoring body (or bodies) must be identified as part of the code and accredited by the competent SA as being capable of effectively monitoring the code. The GDPR does not define the term “accreditation”. However, Article 41 (2) of the GDPR outlines general requirements for the accreditation of the monitoring body. There are a number of requirements, which should be met in order to satisfy the competent supervisory authority to accredit a monitoring body. Code owners are required to explain and demonstrate how their proposed monitoring body meets the requirements set out in Article 41 (2) GDPR to obtain accreditation.

---

<sup>1</sup> References to the “Union” made throughout this opinion should be understood as references to “EEA”.

(4) While the requirements for accreditation of monitoring bodies are subject to the consistency mechanism, the development of the accreditation requirements foreseen in the Guidelines should take into consideration the code's sector or specificities. Competent supervisory authorities have discretion with regard to the scope and specificities of each code and should take into account their relevant legislation. The aim of the Board's opinion is therefore to avoid significant inconsistencies that may affect the performance of monitoring bodies and consequently the reputation of GDPR codes of conduct and their monitoring bodies.

(5) In this respect, the Guidelines adopted by the Board will serve as a guiding thread in the context of the consistency mechanism. Notably, in the Guidelines, the Board has clarified that even though the accreditation of a monitoring body applies only for a specific code, a monitoring body may be accredited for more than one code, provided it satisfies the requirements for accreditation for each code.

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

#### **HAS ADOPTED THE FLOPINION:**

## **1 SUMMARY OF THE FACTS**

1. The Croatian Supervisory Authority (hereinafter "HR SA") has submitted its draft decision containing the accreditation requirements for a code of conduct monitoring body to the Board requesting its opinion pursuant to Art. 64 (1)(c) GDPR, for a consistent approach at Union level. The decision on the completeness of the file was taken on 27 October 2022.
2. In compliance with article 10 (2) of the Board Rules of Procedure, due to the complexity of the matter at hand, the Chair decided to extend the initial adoption period of eight weeks by a further six weeks.

## **2 ASSESSMENT**

### **2.1 General reasoning of the EDPB regarding the submitted draft decision**

3. All accreditation requirements submitted to the Board for an opinion must fully address Art. 41 (2) GDPR criteria and should be in line with the eight areas outlined by the Board in the accreditation section of the Guidelines (section 12, pages 21-25). The Board's opinion aims at ensuring consistency and a correct application of Art. 41 (2) GDPR as regards the presented draft.
4. This means that, when drafting the requirements for the accreditation of a body for monitoring codes according to Art. 41 (3) and 57 (1) (p) GDPR, all the SAs should cover these basic core requirements foreseen in the Guidelines, and the Board may recommend that the SAs amend their drafts accordingly to ensure consistency.

5. All codes covering non-public authorities and bodies are required to have accredited monitoring bodies. Art. 40 (1) GDPR expressly request SAs, the Board and the Commission to “encourage the drawing up of codes of conduct intended to contribute to the proper application of the GDPR, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium sized enterprises”. Therefore, the Board recognises that the requirements need to work for different types of codes, applying to sectors of diverse size, addressing various interests at stake and covering processing activities with different levels of risk.
6. In some areas, the Board will support the development of harmonised requirements by encouraging the SA to consider the examples provided for clarification purposes.
7. When this opinion remains silent on a specific requirement, it means that the Board is not asking the HR SA to take further action.
8. This opinion does not reflect upon items submitted by the HR SA, which are outside the scope of Art. 41 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

## 2.2 Analysis of the HR SA's accreditation requirements for Code of Conduct's monitoring bodies

9. Taking into account that:
  - a. Art. 41 (2) GDPR provides a list of accreditation areas that a monitoring body need to address in order to be accredited;
  - b. Art. 41 (4) GDPR requires that all codes (excluding those covering public authorities as per Art. 41 (6)) have an accredited monitoring body; and
  - c. Art. 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for monitoring bodies and conduct the accreditation of a body for monitoring codes of conduct.

the Board is of the opinion that:

### 2.2.1 GENERAL REMARKS

10. The Board notes that on 22 February 2022, the “Guidelines 04/2021 on Codes of Conduct as tools for transfers” were adopted. These guidelines do not add any additional requirements for the accreditation of monitoring bodies that monitor codes of conduct intended for international transfers. Rather, the guidelines provide further specifications of the general requirements established by Guidelines 1/2019 (Section 12) taking into account the specific context of international transfers.<sup>2</sup> For the sake of clarity, the Board recommends the HR SA to add a reference to the above-mentioned guidelines, which are relevant in the context of monitoring codes of conduct intended for international transfers, for example by amending the last paragraph of the “Introduction” part as follows: “The requirements listed in this document are based on the requirements of Article 41 paragraph (2) of the GDPR and the requirements set out in section 12 of the EDPB Guidelines and taking into account Guidelines 04/2021 on Codes of Conduct as tools for transfers.”

---

<sup>2</sup> See Section 4.2 of the EDPB Guidelines 04/2021 on Codes of Conduct as tools for transfer.

11. As a general remark, the Board recommends that the HR SA amends the definition section in the introductory part of the document to align the definitions contained in the document with those of section 2 of the Guidelines. The Board is of the opinion that the HR SA may use definitions which content is not that of the Guidelines only for terms which are not directly defined in the Guidelines.
12. The Board also believes that the HR SA shall use the same wording as the GDPR where relevant and appropriate.
13. In general terms, the Board also encourages that HR SA to use prescriptive language all across the document. For example, at section 1, as far as translations are concerned, the HR SA shall say that it “will” request a translation instead of “may” request a translation.
14. By way of a general encouragement, the HR SA should correct any typos or formatting errors in the text of the document.
15. The Board has also observed that at section 2.1 of the document titled “General Requirements”, it is stated that “If the Monitoring body is a natural person, it must, in particular, prove that it has the necessary **human** and financial **resources** [...]” and “[...] in the event of an unforeseen event leading to a sudden, temporary or permanent loss of the Monitoring body role, that the monitoring activities may be continued uninterrupted.” The Board encourages the HR SA to specify and further develop those requirements in order for such a monitoring body to be accredited. These requirements could include being able to demonstrate the availability of adequate resources for the specific duties and responsibilities, as well as the full operation of the monitoring mechanism over time. Another example could include the resignation by the person concerned, or his or her temporary inability.

### 2.2.2 APPLICATION REQUIREMENTS

16. With reference to the second minimum information requirement of the application, being that “The Monitoring body’s residence or registered office, which in either case shall be placed in the European Economic Area (EEA)”, the Board recommends that the HR SA specifies, for example by means of a footnote, that monitoring bodies acting in the framework of codes for transfers could be located either inside or also outside of the EEA provided that the concerned monitoring body has an establishment in the EEA.
17. Along the same lines, the Board recommends that HR SA amends the first paragraph of section 2.1 (“General requirements”), which stipulates the following: “The Monitoring body must be a legal entity with a registered office or, if a natural person, have their headquarters or domicile, to exercise the professional activity as a Monitoring body in the European Economic Area (EEA)”. As per the above, monitoring bodies acting in the framework of codes for transfers could be located either inside or also outside of the EEA, provided that the concerned monitoring body has an establishment in the EEA.
18. The Board encourages the HR SA to remove the following sentence in the last paragraph of section 2.1, given that it is redundant with the sentence immediately after: “The Monitoring body must document the principles of its monitoring activities in writing”.
19. For the sake of certainty, the Board also encourages the HR SA to specify that the obligation to provide evidence of the requirements falls upon the monitoring body, and that such evidence must be provided at the application stage.

### 2.2.3 INDEPENDENCE

20. The Board is of the opinion that the independence for a monitoring body should be understood as a series of formal rules and procedures for the appointment, terms of reference and operation of the monitoring body. These rules and procedures will allow the monitoring body to perform the monitoring of compliance with a code of conduct in complete autonomy, without being directly or indirectly influenced, or subjected to any form of pressure that might affect its decisions. This means that a monitoring body should not be in a position to receive any instructions regarding the exercise of its task from code members, the profession, industry or sector to which the code applies, or from the code owner itself.
21. In this regard, the Board notes that paragraph 63 of the Guidelines stipulates that the monitoring body shall be appropriately independent in relation to its impartiality of functions from the code members, the code owner and from the profession, industry or sector to which the code applies. The Board appreciates that the HR SA transposed this requirement into the document. However, the Board recommends that, in order for the text to be consistent with the Guidelines, the HR SA adds the above cited reference to the impartiality of functions.
22. Having read the second paragraph of section 2.2 of the HR SA's accreditation requirements, the Board is of the opinion that such part of the document does not include all the elements which the monitoring body may use as evidence to demonstrate its independence as listed in paragraph 63 of the Guidelines. The Board therefore encourages the HR SA to refer to the monitoring body's funding, the appointment of members/staff, decision making process and more generally to the organisational structure in this respect.
23. In the fourth paragraph of the "Independence" section, the HR SA mentions specifically internal monitoring bodies in relation to their independence. The Board encourages the HR SA to include more details in this respect by adding a reference to the illustrative elements related to the independence of internal monitoring bodies, listed in paragraph 65 of the Guidelines.
24. Having examined section 2.2.1 of the document, titled "Legal and decision-making procedures", the Board acknowledges that the HR SA stipulates that "the duration or expiration of the mandate of the monitoring body must be regulated in such a way to prevent overdependence on a renewal or fear of losing the appointment, to an extent that adversely affects the independence in carrying out the monitoring activities by the Monitoring body." The Board is of the opinion that such a requirement should be expanded by establishing the maximum duration of the term of the monitoring body. In this respect, the Board encourages the HR SA that the maximum duration of the term of the monitoring body should be indicated.
25. The Board is of the opinion that in the last paragraph of section 2.2.1 (the one before the list), the word "pressure" should be replaced with "influence" to be more in line with the spirit of the Guidelines. Hence, the Board encourages the HR SA to amend requirements accordingly.
26. In sub-section 2.2.2, dedicated to the financial resources of the monitoring body, the Board recommends that the HR SA includes a reference to the specific instance where the monitoring body would not be considered to be financially independent if the rules governing its financial support allow a code member, who is under investigation by the monitoring body, to stop its financial contributions to it, in order to avoid a potential sanction from the monitoring body.
27. In respect of financial resources, the Board recommends that the HR SA also adds a specific requirement whereby, in particular in the case of an internal monitoring body, the monitoring body

must prove full autonomy for the management of the budget or other resources. The Board further encourages that the HR SA adds a requirement to prove that the internal monitoring body has a specific separate budget allocated to it by the code owner and which it is able to manage independently.

28. The Board also encourages that, in the same sub-section, the HR SA specifies that the monitoring body must have sufficient financial and other resources together with the necessary procedures to ensure the functioning of the code of conduct over time to ensure long-term financing, i.e. in case one or more funding sources are no longer available.
29. In the matter of organisational resources and structure (sub-section 2.2.3), the HR SA appropriately stated in the document that the monitoring body “must be composed of an adequate and proportionate number of personnel [...].” However, the Board considers that a higher degree of specificity is required in this context and therefore encourages the HR SA to replace the adjective “adequate” with “sufficient numbers of properly qualified personnel”.
30. In addition to the above, in relation to the same requirement related to organisational resources and structure, the Board encourages the HR SA to specify how these aspects could be demonstrated by the monitoring body, for example through the procedure to appoint the monitoring body personnel, the remuneration of the said personnel as well as the duration of the personnel’s mandate and the contract or other formal agreement with the monitoring body.
31. Insofar as internal monitoring bodies are concerned, the HR SA correctly stated in the document that in case such a body is set up within a code owner, the monitoring body must remain structurally separated from the other areas of the code owner’s structure up to and including the level below the senior management. The Board believes that this requirement should be expanded further in line with the Guidelines, and particularly with paragraph 65 thereof. In this respect, the Board encourages the HR SA to specify that the requirements of separate staff and management, accountability and function from other areas of the organisation of an internal monitoring body may be achieved in a number of ways, for example, by putting in place effective organisational and information barriers and separate reporting management structures for the code owner.
32. The Board takes note that the HR SA in the document identified two main ways by means of which the monitoring body can demonstrate its organisational independence. These include, on the one hand, the identification of risks to its organisational independence and how it will remove or minimize such risks and use an appropriate mechanism for safeguarding impartiality, and on the other hand for internal monitoring bodies, setting-up of the organization and information concerning its relationship to its larger entity (i.e., the code owner). In the Board’s view, there are other manners upon which the monitoring body can rely in order to demonstrate its independence, such as for example:
  - the procedure to appoint its personnel;
  - the remuneration of its personnel;
  - the duration of its mandate; and, or
  - contracts or other forms of agreement with the monitoring body.

Thus, the Board encourages the HR SA to include in the document the additional requirements set out above.

#### 2.2.4 CONFLICT OF INTEREST

33. In the section of the document dedicated to “Conflict of interest”, the HR SA appropriately wrote that “in accordance with Article 41 paragraph 2 point (d) of the GDPR, it must be demonstrated that the exercise of the Monitoring body’s tasks and duties do not result in a conflict of interest.” The Board believes that it is the responsibility of the monitoring body to demonstrate this; hence, it encourages the HR SA to re-draft this sentence and amend it accordingly.
34. Furthermore, as far as conflict of interest is concerned, the Board notes paragraph 68 of the Guidelines prescribes that “the monitoring body must remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from any person, organisation or association”. Whilst the Board appreciates that the HR SA stated in the document that the monitoring body must be free of external influence, whether direct or indirect, the Board recommends that the HR SA specifies that the monitoring Body shall neither seek nor take instructions from any person, organisation or association, to fully align the document with the wording of the Guidelines.

#### 2.2.5 EXPERTISE

35. As a general remark, having read sub-section 2.4 of the document on “Expertise”, the Board is of the opinion that this part should contain more details and reflect all the requirements of paragraph 69 of the Guidelines.
36. In particular, the code owners should be able to demonstrate that the monitoring body has the requisite level of expertise to carry out its role in an effective manner. As such, the application will need to include details as to the knowledge and experience of the body in respect of data protection law as well as of the particular sector or processing activity covered by the scope of the code. For example, being able to point to previous experience of acting in a monitoring capacity for a particular sector may assist in meeting this requirement. Furthermore, an in-depth understanding of data protection issues and expert knowledge of the specific processing activities which are the subject matter of the code would be welcomed. The staff of the proposed monitoring body should also have appropriate operational experience and training for carrying out the monitoring of compliance such as in the field of auditing, monitoring, or quality assurance activities. Therefore, the Board recommends that the HR SA amends this sub-section to align it with the wording of paragraph 69 of the Guidelines.
37. The Board notes that the document does not make reference to the legal expertise of the monitoring body, which is also relevant to carry out its monitoring function in an appropriate manner. The Board thus encourages the HR SA to include a requirement specifically on legal expertise. On the other hand, as of technical expertise, the Board encourages that the HR SA specifies that this is also a requirement, depending on the subject-matter of the code to be monitored.

#### 2.2.6 ESTABLISHED PROCEDURES AND STRUCTURES

38. The HR SA included requirements about “Established procedures and structures” in section 2.5 of the document. In the opening of this section, the HR SA refers to “feasible monitoring mechanism”. In view of respecting as much as possible the content of section 12.4 of the Guidelines, the Board encourages that the HR SA replaces this with “appropriate governance and procedures”. Further to this, the Board encourages that the HR SA adds a list of the actions, as presented in paragraph 70 of the Guidelines, which allow the monitoring body to adequately:

- assess for eligibility of controllers and processors to apply the code;
  - monitor compliance with its provisions; and
  - carry out reviews of the code's operation.
39. Further to the above, as of the procedures to actively and effectively monitor code members' compliance with a code's provisions, the Board encourages that the HR SA includes some examples, such as random or unaccounted audits, annual inspections, regular reporting or the use of questionnaires.
40. The Board encourages the HR SA to clarify that the word "expulsion" as used in this paragraph is to be interpreted as "exclusion", which is term used in the GDPR. Furthermore, for the sake of clarity, the Board recommends that in the sentence "The Monitoring body must establish the basis and scope of its activities prior to the start of monitoring tasks to ensure transparency for the Code members and to allow for verification by the Croatian DPA", the word "basis" is deleted.
41. In order to align the document with paragraph 72 of the Guidelines, the Board recommends that the HR SA adds that monitoring procedures can be designed in different ways as long as they take into account factors such as the risks raised by the data processing in scope of the code, complaints received or specific incidents and the number of members of the code etc., and that consideration could be given to the publication of audit reports as well as to the findings of periodic reporting from controllers and processors within the scope of the code.
42. Concerning the requirement in document that "The Monitoring body must establish ad hoc procedures (triggered for example on the basis of an inquiry or complaint from a data subject) to actively and effectively monitor the Code members' compliance with the Code's provisions", the Board recommends that the word "ad hoc" is deleted, given that procedures should be permanent.

### **2.2.7 TRANSPARENT COMPLAINT HANDLING**

43. As for transparent complaint-handling, the Board recommends that the HR SA includes the contents of paragraphs 75 to 77 of the Guidelines in the document. In doing so, the HR SA should adapt the requirements to the wording of the Guidelines. For example, the HR SA should specify that the monitoring body must demonstrate that it has documented procedures and structures to enable it to receive, assess and handle complaints in an impartial and transparent manner.
44. The Board additionally recommends that the HR SA adds a requirement to the document to the effect that the monitoring body needs to have a publicly available complaints-handling process which is sufficiently resourced to manage complaints and to ensure that decisions of the body are made publicly available, as per the relevant part of the Guidelines.
45. Finally, the Board recommends that the HR SA further expands the second paragraph of this section of the document, which reads that "For example, evidence of complaints handling procedure could be a described process to receive, evaluate, track, record and resolve complaints". In the Board's opinion, the HR SA should include the examples given by the Board in the Guidelines in the box between paragraphs 74 and 75 for added clarity.

### **2.2.8 COMMUNICATION WITH THE HR SA**

46. As for the matter of communication with the HR SA, the Board recommends that the contents of the corresponding section of the Guidelines are incorporated in the document. In this regard, the Board

recommends that the first paragraph of section 2.7 of the document is redrafted in alignment with paragraph 78 of the Guidelines by specifying that the actions concerned could include decisions concerning the actions taken in cases of infringement of the code by a code member, providing periodic reports on the code, or providing review or audit findings of the code.

47. The Board additionally recommends that the HR SA makes reference to the effective communication with other competent supervisory authorities and not only with the HR SA, as the case may be and as the need may arise.

#### 2.2.9 CODE REVIEW MECHANISM

48. As a general remark, the Board recommends that section 2.8 is aligned with the corresponding section 12.7 of the Guidelines. Particularly, the Board recommends that the HR SA adds that review mechanisms should also be put in place to adapt to any changes in the application and interpretation of the law or where there are new technological developments which may have an impact upon the data processing carried out by its members or the provisions of the code, as per paragraph 80 of the Guidelines.

#### 2.2.10 LEGAL STATUS

49. With regard to the legal status of the monitoring body, the Board recommends that the HR SA changes the wording to say that instead of “capable of being legally responsible for its monitoring activities”, the monitoring body must be “capable of being fined” to align the wording with paragraph 81 of the Guidelines.
50. Concerning the sentence “The Monitoring body must demonstrate that it is able to deliver the Code of conduct’s monitoring mechanism over a suitable period of time”, the Board encourages the HR SA to replace the word “deliver” with “apply”, which the Board considers more appropriate.
51. The Board encourages the HR SA to specify in the document that the monitoring body can be subject to sanctions by the competent supervisory authority for failing to comply with its obligations, or for failing to act appropriately when the rules of the code of conduct are breached.

### 3 CONCLUSIONS / RECOMMENDATIONS

52. The draft accreditation requirements of the HR SA may lead to an inconsistent application of the accreditation of monitoring bodies and the following changes need to be made.
53. Regarding general remarks, the Board recommends that the HR SA:
  1. adds a reference to the Guidelines 04/2021 on Codes of Conduct as tools for transfers; and
  2. amends the definition section in line with the definitions of the Guidelines.
54. Regarding application requirements, the Board recommends that the HR SA:
  1. specifies, that monitoring bodies acting in the framework of codes for transfers could be located either inside or also outside of the EEA provided that the concerned monitoring body has an establishment in the EEA
  2. amends the first paragraph of section 2.1 in line with the above.

55. Regarding independence, the Board recommends that the HR SA:
1. makes reference to the impartiality of functions as described in paragraph 63 of the Guidelines;
  2. includes a reference to the specific instance whereby the monitoring body would not be considered to be financially independent if the rules governing its financial support allow a code member, who is under investigation by the monitoring body, to stop its financial contributions to it, in order to avoid a potential sanction from the monitoring body; and
  3. adds a specific requirement that, in particular in the case of an internal monitoring body, the monitoring body must prove full autonomy for the management of the budget or other resources.
56. Regarding conflict of interest, the Board recommends that the HR SA specifies that the monitoring body shall neither seek nor take instructions from any person, organisation or association.
57. Regarding expertise, the Board recommends that the HR SA aligns sub-section 2.4 of the draft with the wording of paragraph 69 of the Guidelines.
58. Regarding established procedures and structures, the Board recommends that the HR SA:
1. in the sentence “The Monitoring body must establish the basis and scope of its activities prior to the start of monitoring tasks to ensure transparency for the Code members and to allow for verification by the Croatian DPA”, deletes the word “basis”;
  2. adds that monitoring procedures can be designed in different ways as long as they take into account factors such as the risks raised by the data processing in scope of the code, complaints received or specific incidents and the number of members of the code, etc., and that consideration could be given to the publication of audit reports as well as to the findings of periodic reporting from controllers and processors within the scope of the code; and
  3. deletes the word “ad hoc” with reference to procedures, given that procedures must be permanent.
59. Regarding transparent complaint-handling, the Board recommends that the HR SA:
1. includes the contents of paragraphs 75 to 77 of the Guidelines in the document;
  2. adds a requirement to the document to the effect that the monitoring body needs to have a publicly available complaints-handling process which is sufficiently resourced to manage complaints and to ensure that decisions of the body are made publicly available, as per the relevant part of the Guidelines; and
  3. for added clarity, further expands the second paragraph of this section of the document with the examples given by the Board in the Guidelines in the box between paragraphs 74 and 75.
60. Regarding communication with the HR SA, the Board recommends that the HR SA:
1. incorporates into the document the text of the corresponding section of the Guidelines; and
  2. refers to the effective communication with other competent supervisory authorities and not only with the HR SA, as the case may be and as the need may arise.

61. Regarding code review mechanisms, the Board recommends that the HR SA aligns section 2.8 with the correspondent section of the Guidelines. Particularly, the Board recommends that the HR SA adds that review mechanisms should also be put in place to adapt to any changes in the application and interpretation of the law or where there are new technological developments which may have an impact upon the data processing carried out by its members or the provisions of a code, as per paragraph 80 of the Guidelines.
62. Regarding legal status, the Board recommends that the HR SA changes the sentence reading “capable of being legally responsible for its monitoring activities”, to instead be worded to the effect that the monitoring body must be “capable of being fined”, in order to align the wording with paragraph 81 of the Guidelines.

## 4 FINAL REMARKS

63. This opinion is addressed to the HR SA and will be made public pursuant to Art. 64 (5) (b) GDPR.
64. According to Art. 64 (7) and (8) GDPR, the HR SA shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft decision. Within the same period, it shall provide the amended draft decision or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part. The HR SA shall communicate the final decision to the Board for inclusion in the register of decisions, which have been subject to the consistency mechanism, in accordance with Art. 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

# Opinion of the Board (Art. 64)



**Opinion 03/2023 on the draft decision of the competent supervisory authority of Romania regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR**

**Adopted on 3 February 2023**

## Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT .....	4
2.1	General reasoning of the Board regarding the submitted draft accreditation requirements.	4
2.2	Analysis of the RO SA's accreditation requirements for Code of Conduct's monitoring bodies	5
2.2.1	GENERAL REMARKS .....	5
2.2.2	INDEPENDENCE .....	7
2.2.3	CONFLICT OF INTEREST.....	8
2.2.4	EXPERTISE .....	8
2.2.5	ESTABLISHED PROCEDURES AND STRUCTURES .....	9
2.2.6	TRANSPARENT COMPLAINT HANDLING.....	9
2.2.7	COMMUNICATION WITH THE RO SA .....	9
2.2.8	REVIEW MECHANISMS.....	9
2.2.9	LEGAL STATUS.....	10
3	CONCLUSIONS / RECOMMENDATIONS .....	10
4	FINAL REMARKS.....	12

## **The European Data Protection Board**

Having regard to Article 63, Article 64 (1)(c), (3)-(8) and Article 41 (3) 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 10 and Article 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the European Data Protection Board (hereinafter “the Board”) is to ensure the consistent application of the GDPR when a supervisory authority (hereinafter “SA”) intends to approve the requirements for accreditation of a code of conduct (hereinafter “code”) monitoring body pursuant to article 41. The aim of this opinion is therefore to contribute to a harmonised approach with regard to the suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a code monitoring body by the competent supervisory authority. Even though the GDPR does not directly impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinion by: firstly, requesting the competent SAs to draft their requirements for accreditation of monitoring bodies based on article 41(2) GDPR and on the Board’s “Guidelines 1/2019 on Codes of Conduct and Monitoring bodies under Regulation 2016/679” (hereinafter the “Guidelines”), using the eight requirements as outlined in the guidelines’ accreditation section (section 12); secondly, providing the competent SAs with written guidance explaining the accreditation requirements; and, finally, requesting the competent SAs to adopt the requirements in line with this opinion, so as to achieve an harmonised approach.

(2) With reference to article 41 GDPR, the competent supervisory authorities shall adopt requirements for accreditation of monitoring bodies of approved codes. They shall, however, apply the consistency mechanism in order to allow the setting of suitable requirements ensuring that monitoring bodies carry out the monitoring of compliance with codes in a competent, consistent and independent manner, thereby facilitating the proper implementation of codes across the Union and, as a result, contributing to the proper application of the GDPR.

(3) In order for a code covering non-public authorities and bodies to be approved, a monitoring body (or bodies) must be identified as part of the code and accredited by the competent SA as being capable of effectively monitoring the code. The GDPR does not define the term “accreditation”. However, article 41 (2) of the GDPR outlines general requirements for the accreditation of the monitoring body. There are a number of requirements, which should be met in order to satisfy the competent supervisory authority to accredit a monitoring body. Code owners are required to explain and

---

<sup>1</sup> References to the “Union” made throughout this opinion should be understood as references to “EEA”.

demonstrate how their proposed monitoring body meets the requirements set out in article 41 (2) GDPR to obtain accreditation.

(4) While the requirements for accreditation of monitoring bodies are subject to the consistency mechanism, the development of the accreditation requirements foreseen in the Guidelines should take into consideration the code's sector or specificities. Competent supervisory authorities have discretion with regard to the scope and specificities of each code, and should take into account their relevant legislation. The aim of the Board's opinion is therefore to avoid significant inconsistencies that may affect the performance of monitoring bodies and consequently the reputation of GDPR codes of conduct and their monitoring bodies.

(5) In this respect, the Guidelines adopted by the Board will serve as a guiding thread in the context of the consistency mechanism. Notably, in the Guidelines, the Board has clarified that even though the accreditation of a monitoring body applies only for a specific code, a monitoring body may be accredited for more than one code, provided it satisfies the requirements for accreditation for each code.

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

#### **HAS ADOPTED THE FOLLOWING OPINION:**

## **1 SUMMARY OF THE FACTS**

1. The Romanian Supervisory Authority (hereinafter "RO SA") has submitted its draft decision containing the accreditation requirements for a code of conduct monitoring body to the Board, requesting its opinion pursuant to Art. 64 (1)(c) GDPR, for a consistent approach at Union level. The decision on the completeness of the file was taken on 28 October 2022.
2. In compliance with article 10 (2) of the Board Rules of Procedure, due to the complexity of the matter at hand, the Chair decided to extend the initial adoption period of eight weeks by a further six weeks.

## **2 ASSESSMENT**

### **2.1 General reasoning of the Board regarding the submitted draft accreditation requirements**

3. All accreditation requirements submitted to the Board for an opinion must fully address article 41 (2) GDPR criteria and should be in line with the eight areas outlined by the Board in the accreditation section of the Guidelines (section 12, pages 21-25). The Board opinion aims at ensuring consistency and a correct application of article 41 (2) GDPR as regards the presented draft.
4. This means that, when drafting the requirements for the accreditation of a body for monitoring codes according to articles 41 (3) and 57 (1) (p) GDPR, all the SAs should cover these basic core requirements

foreseen in the Guidelines, and the Board may recommend that the SAs amend their drafts accordingly to ensure consistency.

5. All codes covering non-public authorities and bodies are required to have accredited monitoring bodies. The GDPR expressly request SAs, the Board and the Commission to “encourage the drawing up of codes of conduct intended to contribute to the proper application of the GDPR, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium sized enterprises.” (article 40 (1) GDPR). Therefore, the Board recognises that the requirements need to work for different types of codes, applying to sectors of diverse size, addressing various interests at stake and covering processing activities with different levels of risk.
6. In some areas, the Board will support the development of harmonised requirements by encouraging the SA to consider the examples provided for clarification purposes.
7. When this opinion remains silent on a specific requirement, it means that the Board is not asking the RO SA to take further action.
8. This opinion does not reflect upon items submitted by the RO SA, which are outside the scope of article 41 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

## 2.2 Analysis of the RO SA’s accreditation requirements for Code of Conduct’s monitoring bodies

9. Taking into account that:
  - a. Article 41 (2) GDPR provides a list of accreditation areas that a monitoring body need to address in order to be accredited;
  - b. Article 41 (4) GDPR requires that all codes (excluding those covering public authorities per Article 41 (6)) have an accredited monitoring body; and
  - c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for monitoring bodies and conduct the accreditation of a body for monitoring codes of conduct.

the Board is of the opinion that:

### 2.2.1 GENERAL REMARKS

10. The Board notes that on 22 February 2022, “the Guidelines 04/2021 on Codes of Conduct as tools for transfers” were adopted. These guidelines do not add any additional requirements for the accreditation of monitoring bodies that monitor codes of conduct intended for international transfers. Rather, the guidelines provide further specifications of the general requirements established by the Guidelines 1/2019 (Section 12) taking into account the specific context of international transfers.<sup>2</sup> For the sake of clarity, the Board recommends the RO SA to add a reference to the above-mentioned guidelines, which are relevant in the context of monitoring codes of conduct intended for international transfers.

---

<sup>2</sup> See Section4.2 of the EDPB Guidelines 04/2021 on Codes of Conduct as tools for transfers

11. For the sake of consistency, the Board encourages the RO SA to adjust the terminology used in the requirements to the one used in the Guidelines, this applies in particular to the following terms. The Board also encourages the RO SA to revise the requirements in order to avoid misunderstandings stemming from the translation of the document into English (for example, “criteria for accreditation” should be replaced by “requirements for accreditation”, section 1.4. “Liability” should be replaced by “Accountability”).
12. As regards Section 4 of the draft accreditation requirements, the Board takes into account that paragraph 3 of the draft accreditation requirements is in Romanian language in the submitted draft version of the requirements. The Board, on the basis of the information provided to the Board by the RO SA, understands that the wording of this sentence in English is - “The monitoring procedures can be designed in different ways as long as they take into account factors such as the risks raised by the data processing in scope of the code, complaints received or specific incidents and the number of members of the code.” The Board recommends that the RO SA ensures the inclusion of this paragraph in English, in the final amended version of the requirements.
13. For the sake of consistency and clarity, the Board encourages the RO SA to replace throughout the draft accreditation requirements the term “National Supervisory Authority for Personal Data Processing” with the term “Competent Supervisory Authority” in line with the terminology used in the Guidelines. At the same time the Board encourages the RO SA to rephrase in the definition section of the draft requirements a definition of the term “Competent Supervisory Authority”, to be understood as the National Supervisory Authority for Personal Data Processing.
14. The Board recommends to elaborate the definition of “Accreditation”, so that it is defined in line with the Guidelines, by addition of a last sentence: “The accreditation of a monitoring body applies to a specific code”.
15. The Board notes that the requirements in Section 2 point 3 state that an internal monitoring body “could be an internal department within the code owner”. The Board considers that it should be made explicit that an internal monitoring body cannot be setup within a code member. Therefore, the Board recommends adding a relevant requirement.
16. The Board observes that, Chapter 1 Section 2 paragraph 7 of the requirements mention a renewal of accreditation. However, it is not stated explicitly that in all cases of renewal a repeated evaluation of compliance of the monitoring body with the requirements is carried out. The Board welcomes the provision concerning the re-assessment. However, for the sake of clarity and transparency, the Board recommends the RO SA to explicitly state that in case of substantial changes to the monitoring body relating to the monitoring body’s ability to function independently and effectively, such a review will be always be conducted.
17. The Board notes that Art. 41 GDPR does not refer to the validity of the accreditation of a monitoring body and that there is a margin of manoeuvre for the national SAs. Moreover, the Board notes that the accreditation requirements should be re-assessed periodically, in order to ensure compliance with the GDPR. Indeed, even if the requirements establish a time limit for the accreditation of the monitoring body, this is to be considered without prejudice of the exercise, at any time, of the SA’s supervisory powers with regard to the obligations of the monitoring body. Therefore, for the sake of clarity, the Board encourages the RO SA to clarify that the requirements may be reviewed periodically and to provide transparent information on what happens after the expiry of the validity of the accreditation and what the procedure will be.

## 2.2.2 INDEPENDENCE

18. With respect to the definition of independence, the Board encourages the RO SA to elaborate what independence means. To ensure consistency, such clarification could rely on the wording agreed by the Board in the previous opinions, by specifying that the rules and procedures shall allow the monitoring body to perform the monitoring of compliance with a code of conduct in complete autonomy, without being directly or indirectly influenced or subjected to any form of pressure that might affect its decisions. According to the Board, independence for a monitoring body should be understood as a series of formal rules and procedures for the appointment, terms of reference and operation of the monitoring body. In the Board's view, these rules and procedures will allow the monitoring body to perform the monitoring of compliance with a code of conduct in complete autonomy, without being directly or indirectly influenced, or subjected to any form of pressure that might affect its decisions. This means that a monitoring body should not be in a position to receive any instructions regarding the exercise of its task from code members, the profession, industry or sector to which the code applies, or from the code owner itself. Therefore, the monitoring body must demonstrate impartiality and independence in relation to four main areas: legal and decision-making procedures, financial resources, organisational resources and structure and accountability. In this regard, the Board observes that the RO SA's accreditation requirements do not cover entirely the four areas outlined and are not structured in line with the Guidelines. The Board recommends to elaborate the requirements in line with the Guidelines concerning structure and areas covered. Furthermore, the Board encourages the RO SA to include practical examples that provide a clearer view on how the independence can be demonstrated in the four areas.
19. The Board acknowledges that Subsection 1.2. point 2 in terms of ability to act free from instructions and protected from any sort of sanctions or interference, whether direct or indirect, as a consequence of the fulfilment of its task, the monitoring body is compared to a data protection officer. To avoid confusion and misinterpretation regarding the nature of the monitoring body, the Board encourages to redraft Subsection 1.2., paragraph 2 of the requirements without such a comparison.
20. With regard to Subsection 1.2, paragraph 2 of the draft accreditation requirements, the Board takes note of all the elements demonstrating the monitoring body's independence with respect to its organizational structure. Among others, it is stated that the monitoring body must not be subject to sanctions for the performance of its tasks. The Board considers that it should be further clarified that the monitoring body assumes responsibility for its activities, and it cannot be subject to sanctions by neither the code owner nor the code members. Therefore, the Board encourages the RO SA to redraft this part of the requirements so that the monitoring body is protected, both from the code owner and from the code members, against any dismissal or sanction, direct or indirect, for the performance of its duties.
21. With regard to the financial independence (subsection 1.3. Budget and resources), in the opinion of the Board, the monitoring body would not be considered financially independent if the rules governing its financial support allow a code member, who is under investigation by the monitoring body, to stop its financial contributions to it, in order to avoid a potential sanction from the monitoring body. Therefore, the Board encourages the RO SA to elaborate further this requirement by providing more examples of how the monitoring body can provide such evidence.
22. Regarding subsection 1.3 paragraph 3 on internal monitoring bodies, the Board recommends the RO SA to add a requirement to prove that the internal monitoring body has a specific separated budget that the internal monitoring body is able to manage independently.
23. With regard to the accountability of the monitoring body, the Board notes that the monitoring body should be able to demonstrate "accountability" for its decisions and actions in order to be considered independent. The Board considers that the accountability requirements in subsection 1.4. of the RO SA's

draft accreditation requirements do not fully cover all the elements that should be taken into account. The RO SA should clarify what kind of evidence is expected from the monitoring body, in order to demonstrate accountability. This could be accomplished through such things as setting out roles and decision-making framework and its reporting procedures, and by setting up policies to increase awareness among the staff about the governance structures and the procedures in place. Thus, the Board recommends the RO SA to strengthen the requirements for accountability, to allow for a better understanding of its content in relation to the independence of the monitoring body, and offer examples of the kind of evidence that the monitoring bodies can provide.

### 2.2.3 CONFLICT OF INTEREST

24. As a general remark in this section, the Board is of the opinion that, for practical reasons, examples of cases where a conflict of interest could arise might be helpful. An example of a conflict of interest situation would be the case where personnel conducting audits or making decisions on behalf of a monitoring body had previously worked for the code owner, or for any of the organisations adhering to the code. Therefore, the Board encourages the RO SA to add some examples, similar to the one provided in this paragraph.
25. The Board considers that the measures and procedures in place aiming at preventing conflicts of interest should ensure that the monitoring body shall refrain from any action incompatible with its tasks and duties. Therefore, the Board recommends that the RO SA includes in the accreditation requirements that the procedures and measures in place to avoid conflict of interest ensure that the monitoring body shall refrain from any action incompatible with its tasks and duties.
26. Furthermore, for the sake of consistency and clarity, the Board encourages the RO SA to replace, throughout the draft accreditation requirements, the terms “impartiality” with the term “independence” in line with the terminology used in the Guidelines and keep the term impartiality only in the context of organizational independence of monitoring bodies.

### 2.2.4 EXPERTISE

27. As required by the Guidelines, every code must fulfil the monitoring mechanism criteria (cf. section 6.4 of the Guidelines), by demonstrating “why their proposals for monitoring are appropriate and operationally feasible” (para. 41 of the Guidelines). In this context, all codes with monitoring bodies will need to explain the necessary expertise level for their monitoring bodies in order to deliver the code’s monitoring activities effectively. Section 3 of the RO SA draft accreditation requirements refers to the “appropriate level of expertise necessary to perform its role effectively”. A reference to the level of experience as required by the code itself is missing. The Board encourages the RO SA to add examples so that the data protection expertise, experience and knowledge required, are reflected in the code itself.
28. The Board agrees with the RO SA that expertise needs to involve the subject-matter (sector) of the code, in which case the relevant requirements that must be fulfilled can be specific, based on the sector to which the code applies. In this context, the Board recommends clarifying section 3 paragraph 2 that different interests involved and the risks of the processing activities addressed by the code should also be taken into account.
29. Moreover, the Board notes that RO SA’s expertise requirements do not differentiate between staff at the management level and, therefore, in charge of the decision-making process, and staff at the operating level, conducting the monitoring activities. In this regard, the Board encourages the RO SA to clarify in

section 3 which requirement should be met by the staff performing the monitoring function and the personnel making the decisions.

#### 2.2.5 ESTABLISHED PROCEDURES AND STRUCTURES

30. As regards Section 4 of the draft accreditation requirements, the Board notes that paragraph 3 of the draft accreditation requirements states that: "The monitoring procedures can be designed in different ways as long as they take into account factors such as the risks raised by the data processing in scope of the code, complaints received or specific incidents and the number of members of the code." The Board observes that the essence of the requirements is in line with the paragraph 72 of the Guidelines. However, the Board considers that the consideration in section 4 paragraph 4 of the requirements is meant as an example. Therefore, for the sake of clarity and consistency, the Board encourages to distinguish the requirements that are meant as examples of possible ways to comply with the requirements from the requirements themselves. The Board also recommends to add some examples in the requirements, such as random or unannounced audits, annual inspections, regular reporting and the use of questionnaires.
31. With regard to section 4. Paragraph 5, the Board notes that the procedure to ensure the monitoring of the code of conduct will take into account the "number of code members". Since the number of code members may not be known at the moment the monitoring body applies for accreditation, the Board encourages the RO SA to refer to the expected number and size of the code members.

#### 2.2.6 TRANSPARENT COMPLAINT HANDLING

32. Regarding the complaints about code members (Section 5 of the RO SA accreditation requirements), the Board acknowledges that complaints handling process requirements should be set at a high level and contain reasonable time frames for answering complaints. Thus, the Board recommends the RO SA to take a more flexible approach, by stating that the monitoring body will have to provide the complainant with progress reports or the outcome within a reasonable timeframe, such as three months.
33. Regarding Section 5 paragraph 2 of the RO SA's draft accreditation requirements, the Board considers that under section 74 of the Guidelines, the requirements related to the complaint handling process should contain the obligation of the monitoring body to make its decisions or general information thereof, publicly available. The Board notes that the wording of the accreditation requirements currently only addresses the need to ensure availability of sufficient resources to ensure that decisions are made publicly available. Therefore, the Board recommends that the requirement is redrafted to include a obligation for the monitoring body to make decision publicly available.

#### 2.2.7 COMMUNICATION WITH THE RO SA

34. The Board notes that Heading of Section 6 contains a reference to the competent supervisory authority. Considering that this section covers the communication with the RO SA, for the sake of clarity and consistency the Board recommends that "Competent supervisory authority" should be replaced by reference to "National Supervisory Authority for Personal Data Processing".

#### 2.2.8 REVIEW MECHANISMS

35. With regard to section 7 of the RO SA's draft accreditation requirements, the Board notes that the reference to the periodic review does not mention that the SA will review the compliance with the

requirements periodically. Thus, the Board encourages the RO SA to clarify that the requirements may be reviewed periodically and to provide transparent information on how the periodic review will work in practice and what happens after the expiry of the validity of the accreditation.

36. The Board notes that under section 7.2 of the requirements there is no reference to the fact that the updating of the code of conduct is the responsibility of the code owner. The Board is of the opinion that, in order to avoid confusion, a reference to the code owner should be made. Therefore, the Board encourages the RO SA to amend this section accordingly so to include such a reference to the code owner.

#### 2.2.9 LEGAL STATUS

37. The code of conduct itself will need to demonstrate that the operation of the code's monitoring mechanism is sustainable over time, covering worst-case scenarios, such as the monitoring body being unable to perform the monitoring function. In this regard, it would be advisable to require that a monitoring body demonstrates that it can deliver the code of conduct's monitoring mechanism over a suitable period of time. The financial, human and material resources to ensure the continuity of the monitoring body should be accompanied with the necessary procedures to ensure the functioning of the monitoring mechanism over a suitable time. Therefore, the Board recommends RO SA to explicitly require that monitoring bodies shall demonstrate continuity of the monitoring function over time. The Board also encourages the RO SA to include in the accreditation requirements that, in order to demonstrate the continuity of the monitoring function, the monitoring body should demonstrate that it has sufficient financial and other resources, and the necessary procedures.
38. The Board notes that the RO SA's requirements or explanatory notes do not reference subcontracting, leaving this area open for monitoring bodies applying for accreditation to decide upon. The Board recommends that RO SA clarifies whether the monitoring body may have recourse to subcontractors, on which terms and conditions and that these are reflected in the explanatory notes or ordinance accordingly. If RO SA indicates that subcontracting is allowed, the Board recommends that the RO SA indicates, in the requirements, that the obligations applicable to the monitoring body are applicable in the same way to subcontractors.
39. The Board observes that section 8 paragraph 4 requires the monitoring board to have a premises in the EEA. The Board is of the opinion that a monitoring body requires an establishment in the EEA. This is to ensure that they can uphold data subject rights, deal with complaints and that GDPR is enforceable and also ensures supervision by the SA. The Board encourages that RO SA clarify that the premises of monitoring body are to be understood as an establishment in the EEA.

### 3 CONCLUSIONS / RECOMMENDATIONS

40. The draft accreditation requirements of the RO Supervisory Authority may lead to an inconsistent application of the accreditation of monitoring bodies and the following changes need to be made:
41. Regarding general remarks, the Board recommends that the RO SA:
1. adds a reference to Guidelines 04/2021, which are relevant in the context of monitoring codes of conduct intended for international transfers.
  2. elaborates the definition of "Accreditation", by addition of a last sentence with the following wording: "The accreditation of a monitoring body applies to a specific code".

3. clarifies in the text of the requirements that internal monitoring bodies cannot be set up within a code member, but only within a code owner.
4. Explicitly state that in case of substantial changes to the monitoring body relating to the monitoring body's ability to function independently and effectively, a review of the body that ensures that the monitoring body still meets the requirements for accreditation will be always conducted.

42. Regarding independence the Board recommends that the RO SA:

1. further develops the requirements, in line with the four areas, for example ;
2. to add a requirement to prove that the internal monitoring body has a specific separated budget;
3. strengthens the requirements for accountability in the draft requirements, to allow for a better understanding of its content in relation to independence of the monitoring body, and offer examples of the kind of evidence that the monitoring body can provide.

43. Regarding conflict of interest the Board recommends that the RO SA:

1. includes in the accreditation requirements that the procedures and measures in place to avoid conflict of interest ensure that the monitoring body shall refrain from any action incompatible with its tasks and duties.

44. Regarding expertise the Board recommends that the RO SA:

1. clarifies that other factors such as the size of the sector concerned, the different interests involved and the risks of these processing activities should be taken into account, in order to assess the level of expertise of the monitoring body.

45. Regarding established procedures and structure the Board requires that the RO SA:

1. adds some examples in the requirements, such as random or unannounced audits, annual inspections, regular reporting and the use of questionnaires. In addition, the monitoring procedures can be designated in different ways as long as they take into account factors such as the risks raised by the data processing within the scope of a code, complaints received or specific incidents and the number of members of a code.

46. Regarding transparent complaint handling the Board requires that the RO SA:

1. takes a more flexible approach, by stating that the monitoring body will have to provide the complainant with progress reports or the outcome within a reasonable timeframe, such as three months.
2. aligns the text of the accreditation requirements with the Guidelines, in order to ensure that the decisions, or general information thereof, are publicly available.

47. Regarding communication with the RO SA the Board requires that the RO SA:

1. In the heading of the Section 6 replaces "Competent supervisory authority" with "National Supervisory Authority for Personal Data Processing".

48. Regarding the legal status the Board requires that the RO SA:

1. explicitly requires that monitoring bodies demonstrate continuity of the monitoring function over time;

2. clarifies whether the monitoring body may have recourse to subcontractors and on which terms and conditions and that these are reflected in the requirements or explanatory notes. If subcontracting is allowed, amend the requirements or explanatory notes, so that the obligations applicable to the monitoring body are applicable in the same way to subcontractors.

## 4 FINAL REMARKS

49. This opinion is addressed to the Romanian supervisory authority and will be made public pursuant to Article 64 (5) (b) GDPR.
50. According to Article 64 (7) and (8) GDPR, the RO SA shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft decision. Within the same period, it shall provide the amended draft decision or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.
51. The RO SA shall communicate the final decision to the Board for inclusion in the register of decisions, which have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

# Opinion of the Board (Art. 64)



**Opinion 4/2023 on the draft decision of the competent supervisory authority of Malta regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)**

**Adopted on 3 February 2023**

## Table of contents

1	Summary of the Facts.....	4
2	Assessment .....	4
2.1	General reasoning of the EDPB regarding the submitted draft decision.....	4
2.2	Main points of focus for the assessment (art. 43.2 GDPR and Annex 1 to the EDPB Guidelines) that the accreditation requirements provide for the following to be assessed consistently:.....	5
2.2.1	PREFIX .....	6
2.2.2	GENERAL REMARKS.....	6
2.2.3	GENERAL REQUIREMENTS FOR ACCREDITATION .....	6
2.2.4	RESOURCE REQUIREMENTS .....	8
2.2.5	PROCESS REQUIREMENTS .....	9
3	Conclusions / Recommendations .....	10
4	Final Remarks .....	11

## The European Data Protection Board

Having regard to Article 63, Article 64 (1c), (3) - (8) and Article 43 (3) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereafter “GDPR”),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,<sup>1</sup>

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

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (hereafter GDPR) throughout the European Economic Area. In compliance with Article 64.1 GDPR, the Board shall issue an opinion where a supervisory authority (SA) intends to approve the requirements for the accreditation of certification bodies pursuant to Article 43. The aim of this opinion is therefore to create a harmonised approach with regard to the requirements that a data protection supervisory authority or the National Accreditation Body will apply for the accreditation of a certification body. Even though the GDPR does not impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by encouraging SAs to draft their requirements for accreditation following the structure set out in the Annex to the EDPB Guidelines on accreditation of certification bodies, and, secondly by analysing them using a template provided by EDPB allowing the benchmarking of the requirements (guided by ISO 17065 and the EDPB guidelines on accreditation of certification bodies).

(2) With reference to Article 43 GDPR, the competent supervisory authorities shall adopt accreditation requirements. They shall, however, apply the consistency mechanism in order to allow generation of trust in the certification mechanism, in particular by setting a high level of requirements.

(3) While requirements for accreditation are subject to the consistency mechanism, this does not mean that the requirements should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB opinion is not to reach a single EU set of requirements but rather to avoid significant inconsistencies that may affect, for instance trust in the independence or expertise of accredited certification bodies.

(4) The “Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)” (hereinafter the “Guidelines”), and “Guidelines 1/2018 on certification and identifying certification criteria in accordance with article 42 and 43 of the Regulation 2016/679” will serve as a guiding thread in the context of the consistency mechanism.

(5) If a Member State stipulates that the certification bodies are to be accredited by the supervisory authority, the supervisory authority should establish accreditation requirements including, but not

---

<sup>1</sup> References to the “Union” made throughout this opinion should be understood as references to “EEA”.

limited to, the requirements detailed in Article 43(2). In comparison to the obligations relating to the accreditation of certification bodies by national accreditation bodies, Article 43 provides fewer details about the requirements for accreditation when the supervisory authority conducts the accreditation itself. In the interests of contributing to a harmonised approach to accreditation, the accreditation requirements used by the supervisory authority should be guided by ISO/IEC 17065 and should be complemented by the additional requirements a supervisory authority establishes pursuant to Article 43(1)(b). The EDPB notes that Article 43(2)(a)-(e) reflect and specify requirements of ISO/IEC 17065 which will contribute to consistency.<sup>2</sup>

(6) The opinion of the EDPB shall be adopted pursuant to Article 64 (1)(c), (3) & (8) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

## **HAS ADOPTED THE OPINION:**

### **1 SUMMARY OF THE FACTS**

1. The Office of the Information and Data Protection Commissioner (hereinafter “MT SA”) has submitted its draft accreditation requirements under Art. 43 (1)(b) GDPR to the EDPB. The file was deemed complete on 27 October 2022. The National Accreditation Board (Malta), as national accreditation body (NAB), will perform accreditation of certification bodies to certify the use of GDPR certification criteria. This means that the NAB will use ISO/IEC 17065 and the additional requirements set out by the MT SA, once they are approved by the MT SA, following an opinion from the Board on the draft requirements, to accredit certification bodies.
2. In compliance with article 10 (2) of the Board Rules of Procedure, due to the complexity of the matter at hand, the Chair decided to extend the initial adoption period of eight weeks by a further six weeks.

### **2 ASSESSMENT**

#### **2.1 General reasoning of the EDPB regarding the submitted draft decision**

3. The purpose of this opinion is to assess the accreditation requirements developed by a SA, either in relation to ISO 17065 or a full set of requirements, for the purposes of allowing a national accreditation body or a SA, as per Art. 43(1) GDPR, to accredit a certification body responsible for issuing and renewing certification in accordance with Art. 42 GDPR. This is without prejudice to the tasks and powers of the competent SA. In this specific case, the Board notes that the Maltese national law prescribes that its NAB is responsible for the issuance of accreditation. The MT SA has therefore drafted additional requirements in accordance with the Guidelines, which should be used by its NAB

---

<sup>2</sup> Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation, para. 39. Available at: [https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies\\_en](https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_en)

when issuing accreditation. To this end, the MT SA has developed a set of requirements specifically for accreditation of certification bodies in conjunction with a set of certification criteria that is yet to be formally approved.

4. This assessment of MT SA's additional accreditation requirements is aimed at examining on variations (additions or deletions) from the Guidelines and notably their Annex 1. Furthermore, the EDPB's Opinion is also focused on all aspects that may impact on a consistent approach regarding the accreditation of certification bodies.
5. It should be noted that the aim of the Guidelines on accreditation of certification bodies is to assist the SAs while defining their accreditation requirements. The Guidelines' Annex does not constitute accreditation requirements as such. Therefore, the accreditation requirements for certification bodies need to be defined by the SA in a way that enables their practical and consistent application as required by the SA's context.
6. The Board acknowledges the fact that, given their expertise, freedom of manoeuvre should be given to NABs when defining certain specific provisions within the applicable accreditation requirements. However, the Board considers it necessary to stress that, where any additional requirements are established, they should be defined in a way that enables their practical, consistent application and review as required.
7. The Board notes that ISO standards, in particular ISO/IEC 17065, are subject to intellectual property rights, and will therefore not refer to the text of the related document in this Opinion. As a result, the Board decided to, where relevant, point towards specific sections of the ISO Standard, without, however, reproducing the text.
8. Finally, the Board has conducted its assessment in line with the structure foreseen in Annex 1 to the Guidelines (hereinafter "Annex"). Where this Opinion remains silent on a specific section of the MT SA's draft accreditation requirements, it should be read as the Board not having any comments and not asking the MT SA to take further action.
9. This Opinion does not reflect upon items submitted by the MT SA, which are outside the scope of Art. 43 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

## 2.2 Main points of focus for the assessment (art. 43.2 GDPR and Annex 1 to the EDPB Guidelines) that the accreditation requirements provide for the following to be assessed consistently:

- a. addressing all the key areas as highlighted in the Guidelines Annex and considering any deviation from the Annex.
- b. independence of the certification body
- c. conflicts of interests of the certification body
- d. expertise of the certification body
- e. appropriate safeguards to ensure GDPR certification criteria is appropriately applied by the certification body
- f. procedures for issuing, periodic review and withdrawal of GDPR certification; and

- g. transparent handling of complaints about infringements of the certification.
10. Taking into account that:
- a. Article 43 (2) GDPR provides a list of accreditation areas that a certification body need to address in order to be accredited;
  - b. Article 43 (3) GDPR provides that the requirements for accreditation of certification bodies shall be approved by the competent Supervisory Authority;
  - c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for certification bodies and may decide to conduct the accreditation of certification bodies itself;
  - d. Article 64 (1) (c) GDPR provides that the Board shall issue an opinion where a supervisory authority intends to approve the accreditation requirements for a certification body pursuant to Article 43(3);
  - e. If accreditation is carried out by the national accreditation body in accordance with ISO/IEC 17065/2012, the additional requirements established by the competent supervisory authority must also be applied;
  - f. Annex 1 of the Guidelines on Accreditation of Certification foresees suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a certification body by the National Accreditation Body;
- the Board is of the opinion that:
- ### 2.2.1 PREFIX
11. The Board acknowledges the fact that terms of cooperation regulating the relationship between a NAB and the SA are not a requirement for the accreditation of certification bodies *per se*. However, for reasons of completeness and transparency, the Board considers that such terms of cooperation, where existing, shall be made public in a format considered appropriate by the SA.
- ### 2.2.2 GENERAL REMARKS
12. Under the section “terms and definitions” the Board notes that the draft accreditation requirements state that terms and definitions of the EDPB Guidelines on accreditation and Guidelines on certification shall apply and have precedence over ISO definitions, but there is no reference to the definitions used for the same concepts in the GDPR. Thus, the Board recommends the MT SA to also include reference to the terms and definitions of the GDPR.
13. For completeness and consistency purposes, the Board encourages the MT SA to make sure that throughout the requirements the term “target of evaluation” is used in order to ensure clear and consistent wording thorough the text.
- ### 2.2.3 GENERAL REQUIREMENTS FOR ACCREDITATION

14. Concerning subsection 4.1.1 of the MT SA's draft accreditation requirements (Legal responsibility), the Board considers that the certification body shall be able to demonstrate evidence of GDPR compliant procedures and measures specifically for controlling and handling client organisation's personal data as part of the certification process. To that end, the Board notes that MT SA refers only to the "applicant" (no reference to the "client" is made), which may be confusing as the same criteria should be applicable for the renewal of accreditation. Therefore, the Board recommends that the MT SA amends the draft requirements accordingly.
15. Also, in this subsection (Legal responsibility), the Board notes the requirement for the certification body to confirm with the NAB that they are not subject to any investigation or regulatory action by the MT SA in relation to the target of evaluation, which may mean that they do not meet this requirement and therefore might prevent their accreditation. This requirement further on provides some ambiguity when it does not give clear criteria (saying "where appropriate") on the situations in which the NAB may contact the MT SA in order to verify this information. To that end, the Board recommends to the MT SA to ensure further clarification and specify clear conditions for this procedure.
16. In addition to that, the Board is of the opinion that subsection 4.1.1 of the MT SA's draft accreditation requirements, regarding the obligation of the certification body to inform the NAB of "any" infringements of the GDPR or of national data protection legislation which may affect its accreditation, should be further clarified, taking into account the above-mentioned requirement that certification body should confirm to the NAB that they are not subject to any investigation or regulatory action by the MT SA in relation to the target of evaluation. Thus, the Board considers that this obligation should refer to infringements established by the MT SA and/or judicial authorities and recommends the MT SA to makes such clarification.
17. Further on, concerning subsection 4.1.1 of the MT SA's draft accreditation requirements, the Board notes that the certification body shall be required to inform the MT SA prior to issuing or renewing a certification and to that end, requirements are referring to Art. 43(1) GDPR. At the same time, the Board notes that the MT SA's draft accreditation requirements in point 7.6 further elaborate this requirement for the certification body. Thus, the Board encourages the MT SA to include in this subsection the reference on the last sentence of point 7.6 of the accreditation requirements, in addition to the already existing one related to Art. 43(1) GDPR.
18. Under section 4.1.2 (i) of the MT SA's draft accreditation requirements, the Board takes note of the obligation to explain the consequences of withdrawal or suspension of accreditation for the certification body and how this impacts the client. The Board understands that the intention of the MT SA is to ensure that the client is aware of the consequences in those situations and of the potential options or actions that can be taken. However, the Board considers that, in order to ensure that certification agreements accurately reflect not only the consequences and impacts on the client, but also the potential further actions, the MT SA's accreditation requirements should make clear that simply stating the consequences without addressing the potential next steps will not be sufficient. Thus, the EDPB encourages the MT SA to make clear in its accreditation requirements that the clients should be aware of the consequences, the impact they have on them and the potential next steps that may be taken.
19. Regarding section 4.1.2 (j) of the MT SA's accreditation requirements, the Board notes the inclusion of the requirement to inform the certification body in the event of significant changes in its factual or legal situation and in its processing operations covered by the certification. However, the MT SA

omitted a reference to “products, processes and services”, as stated in the Annex. The Board therefore recommends the MT SA to align the wording with the Annex.

20. Regarding the requirements related to the content of the Certification agreement listed in section 4.1.2, the Board notes that point 10 of section 4.1.2. of the Annex, as reflected in point 4.1.2 (j) of the MT SA’s draft requirements, requires the applicant to inform the certification body in the event of significant changes in its actual or legal situation and in its products, processes and services concerned by the certification. The Board considers that these changes shall include the obligation of the applicant to inform the certification body of any infringements of the GDPR established by the MT SA and/or judicial authorities that may affect certification. Indeed, such requirement is foreseen further in the text of the requirements (section 7.10 (e) of the requirements). However, for the sake of clarity, the Board recommends to the MT SA to include explicitly this point in this section of the requirements.
21. With respect to the section 4.2 “Management of impartiality”, the Board notes the obligation to lay down rules preventing conflicts of interest. The Board acknowledges the importance to have requirements that ensure, firstly, that there are no conflicts of interests and, secondly, in case conflicts of interest are identified, that the certification body manages them. Therefore, the Board encourages the MT SA to clarify that, in addition to having rules preventing conflicts of interest, there should be clear rules to manage identified conflicts of interests.
22. Regarding section 4.6 of the MT SA’s draft accreditation requirements, the certification body is required to:
  - a. publish and make easily publicly available all versions (current and previous) of the approved criteria used within the meaning of Art. 42(5) GDPR, as well as all certification procedures, generally stating the respective period of validity; and
  - b. provide information about complaints handling procedures and appeals is transparent to data subjects and the public pursuant to Art. 43(2)(d) GDPR.The Board recommends to the MT SA to add in the requirements that this information shall be provided at minimum, according to section 4.6 of the ISO/IEC 17065/2012 and in line with section 4.6 of the Annex.
23. In order to avoid inaccuracies, possible different understandings and interpretations of the requirement for publicly available information relating to complaint handling procedures and appeals, the Board recommends to the MT SA to align the wording of section 4.6 (b) of the MT SA’s draft accreditation requirement with the Annex.

#### 2.2.4 RESOURCE REQUIREMENTS

24. Regarding section 6.1 (f) of the MT SA’s draft accreditation requirements, with respect to the second bullet point of the subsection relating to the personnel with technical expertise, the Board refers to the sentence by which it is prescribed that “personnel responsible for certification decisions shall demonstrate at least two years professional experience in data protection law”. Considering this section of requirements is addressed to the personnel with technical expertise, the Board consider reference to experience in data protection “law” inaccurate and recommends the MT SA to align the wording with the Annex.
25. Also, regarding section 6.1 (f) of the MT SA’s draft accreditation requirements, with respect to the third bullet point of the subsection relating to the personnel with legal expertise, the Board refers to

the sentence by which it is prescribed that “personnel responsible for evaluations must demonstrate at least two years of professional experience in data protection law and knowledge and experience in technical data protection”. Considering this section of requirements is addressed to the personnel with legal expertise the Board consider reference to “experience in technical data protection” inaccurate and recommends the MT SA to align the wording with the Annex.

26. As regards the requirements for personnel responsible for evaluations, in subsection related to personnel with technical expertise, the Board recommends the MT SA to refer to professional experience in “technical” data protection.

## 2.2.5 PROCESS REQUIREMENTS

27. Taking into account that section 7 of the MT SA’s draft accreditation requirements concerns process requirements and sets certain requirements for the NAB, the Board encourages the MT SA to rephrase section 7.1 (d) in such a way as to replace the words “carries out an investigation” with “have established procedures to investigate”.
28. The Board notes that section 7.2 of the MT SA’s draft accreditation requirements (“Application”) concerns obligations imposed on the applicants towards the certification body. To that end, the Board recommends to the MT SA to rephrase the first paragraph of this section as follows: “In addition to clause 7(2) of ISO 17065, the certification body shall require from the applicant to [...]”
29. The Board notes that section 7.2 of the MT SA’s draft accreditation requirements (“Application”) contains a reference to the controller/processor contract(s) and their specific arrangements. While acknowledging that the MT SA has used the wording of the Annex, the Board encourages the MT SA to include a reference to joint controllers and their specific arrangements.
30. Furthermore, the Board recommends to the MT SA to rephrase the section 7.2 (c) in a way to delete the reference to “the certification body” so that it is clear from the text that this obligation primarily refers to the applicant’s obligation during the application stage and fulfilment of which should be checked by the certification body.
31. Regarding section 7.2 (c) (“Application”) of the MT SA’s draft accreditation requirements, the Board notes that it includes the obligation to provide information regarding “any current investigation or regulatory action of the Malta SA to which the applicant is or has been subject”. The Board is of the opinion that this obligation should be tailored to investigations or regulatory actions related to the scope of the certification and the target of evaluation. Therefore, the Board encourages the MT SA to clarify that the investigation or regulatory action should be related to the scope of certification and the target of evaluation.
32. The Board notes that the clarification on the requirement relating to the data protection certification in accordance with Art. 42 and 43 GDPR, which already covers part of the object of certification, according to which “a certification statement or similar certification certificates should not be considered sufficient to replace a report” (section 7.4 of the Annex) is not included in the MT SA’s draft requirements. Thus, the Board recommends that the MT SA includes it in the requirement.
33. Concerning third paragraph of the section 7.6 of the MT SA’s draft accreditation requirements (“Certification decision”), the Board notes that the certification body shall be required, in addition to the checks carried out at application stage, prior to issuing certification, to confirm with the applicant that they are not the subject of any investigation or regulatory action by the MT SA, by any other

supervisory authority and, or by competent judicial authorities in relation to the object of the certification which might prevent certification being issued. Further in the text it is foreseen that the applicant's statement can be confirmed with the MT SA not only prior to issuing, but also prior to the renewing of certification. Therefore, the Board encourages that the MT SA amends this inconsistency.

34. Regarding first paragraph of the section 7.8 of the MT SA's draft accreditation requirements ("Directory of certified product") the Board notes the requirement that records of the certifications issued, including information about the certification mechanism and how long the certifications are valid for shall be publicly available and thus, in principle, it could be concluded that this implies an requirement to keep this information also internally but at the same time, for the purpose of consistency and clarity, Board encourages MT SA to align the wording with the Annex.
35. In addition, the Board notes that this section contains clear requirements aimed at helping with transparency on what has been certified and how it was assessed, to that end, for the purpose of clarity and alignment with Annex the Board encourages the MT SA to delete the words "on which basis" from the first paragraph of the section 7.8.
36. In order to ensure clarity, the Board encourages the MT SA to align the wording in section 7.10 (c) and (d) of the draft accreditation requirements with the Annex.

### 3 CONCLUSIONS / RECOMMENDATIONS

37. The draft accreditation requirements of the MT Supervisory Authority may lead to an inconsistent application of the accreditation of certification bodies and the following changes need to be made:
38. Regarding 'general remarks', the Board recommends that the MT SA:
  - 1) includes references to the terms and definitions of the GDPR
39. Regarding 'general requirements for accreditation', the Board recommends that the MT SA:
  - 2) amend subsection 4.1.1 in line with the remarks made in paragraphs 13 and 14 of the Opinion;
  - 3) makes clarification in subsection 4.1.1 of the draft accreditation requirements that the obligation of the certification body to inform the NAB on infringements of the GDPR should refer to infringements established by the MT SA and/or judicial authorities in relation to the target of evaluation;
  - 4) align the wording of section 4.1.2 (j) of the accreditation requirements with the Annex;
  - 5) include the point relating to applicant informing the certification body of any infringements of the GDPR established by the MT SA and/or judicial authorities that may affect certification in subsection 4.1.2 of the requirements;
  - 6) align the wording of section 4.6 (b) with the Annex.
40. Regarding 'resource requirements', the Board recommends that the MT SA:
  - 1) align the wording of second bullet point of the section 6.1 (f) relating to the personnel with technical expertise with the Annex;

- 2) align the wording of third bullet point of the section 6.1 (f) relating to the personnel with legal expertise with the Annex;
  - 3) align the wording of third bullet point of the section 6.1 (f) of the subsection relating to the personnel with technical expertise with the Annex.
41. Regarding 'process requirements', the Board recommends that the MT SA:
- 1) amend section 7.2 in line with the remarks made in paragraphs 27 and 29 of this Opinion
  - 2) to include in draft accreditation requirements the sentence of section 7.4 of the Annex which stipulates that "a certification statement or similar certification certificates should not be considered sufficient to replace a report".
  - 3) amend section 7.6, third paragraph of the draft accreditation requirements in a way which clearly points that the intended procedure applies also to the renewing of certification.

## 4 FINAL REMARKS

42. This opinion is addressed to the MT SA and will be made public pursuant to Art. 64 (5)(b) GDPR.
43. According to Art. 64 (7) and (8) GDPR, the MT SA shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft decision. Within the same period, it shall provide the amended draft decision or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.
44. The MT SA shall communicate the final decision to the Board for inclusion in the register of decisions, which have been subject to the consistency mechanism, in accordance with Art. 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

## Annex: National Reports on the CEF cloud action

## Table of Contents

AT SA .....	3
BE SA ..	8
CY SA ..	15
CZ SA ..	19
DE SA ..	23
EDPS ..	32
EE SA ..	41
EL SA ..	46
ES SA ..	57
FI SA ..	62
IS SA ..	67
IT SA ..	72
LI SA ..	83
LT SA ..	91
NL SA ..	99
PT SA ..	107
SE SA ..	112
SI SA ..	116
SK SA ..	122

# AT SA

## Part I – Statistics

### 1. Which stakeholders have you contacted under the coordinated action?

- Federal Ministry of Education, Science and Research

### 2. How many stakeholders have you contacted within the following categories?

- Ministry of the central government: **One, see Q1.**
- Independent public body of the central government
- Buyer for the central government
- Publicly-owned company acting as a processor for several central public bodies
- Ministry of the regional government
- Independent public body of the regional government
- Buyer for the regional government
- Publicly-owned company acting as a processor for several regional public bodies
- Other, please specify

### 3. How many stakeholders have you contacted within the following sectors?

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government
- Economic affairs
- Education: **One, see Q1.**
- Finance
- Health
- Infrastructure
- Employment
- Justice
- Tax
- Other, please specify

### 4. If you have contacted a buyer, for which sectors does this buyer provides its services?

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government
- Economic affairs
- Education
- Finance
- Health
- Infrastructure
- Employment
- Justice
- Tax
- No specific sector
- Other, please specify

- Answer: N/A

**5. If you have contacted a buyer, please specify the number of stakeholders this buyer provides services for?**

- N/A

**6. What was the initial procedural framework of your action?**

- Fact finding
- Fact finding + determining follow-up action based on the results
- New investigation: **Started a new investigation**
- Ongoing investigation

**7. How many stakeholders indicated that they use CSPs or are planning to do so in the near future (end of 2022)?**

- One, see Q1.

**8. Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?**

- Internal organisation (office suites, internal communication, HR, etc.) : **One, see Q1, in-house-Communication**
- Exercise of public functions (services to citizens, processing citizen's data, etc.): **One, see Q1, Communication**

**9. For the following commonly identified sectors, please specify if any hyperscalers are involved (if so please name them) - N/A**

- Health
- Finance
- Tax
- Education
- Central buyers or providers of IT services

**10. How many stakeholders took the following actions prior to- or during the acquisition of a CSP?**

- Perform a DPIA
- Does the DPIA analyses transfers in details (sometimes called DTIA)
- Perform a general risk analysis: **One, see Q1.**
- Contact the DPO for advice: **One, see Q1.**
- Contact the SA for advice

**11. How many stakeholders (including buyers) take the following actions during the use of the CSP?**

- Monitoring technical and organisational measures to ensure compliance
- In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g. Schrems II): **One, see Q1**
- Regular risk assessments: **One, see Q1.**

## **Part II – Substantive issues**

**1. Pre-contractual phase**

**1.1. Briefly describe the main issue(s) identified.**

- Question whether DPIA would need to be carried out.

- Three offers have been evaluated esp. regarding the least processing of personal data required by the cloud provider

**1.2. Which provision(s) of the GDPR (or national laws) does this concern?**

- Art. 35 GDPR
- Chapter II

**1.3. Explain why this has been an issue for your stakeholders?**

- Public bodies feared questions of possible liability, even though they ultimately deemed no DPIA to be necessary.

**1.4. What are differences that you have encountered between stakeholders in your Member State?**

- -

**1.5. What are solutions to this issue? Please describe if these solutions are already implemented or potential, and whether this solution is provided by the SA or the stakeholders.**

- Concerning Data Processing on this scale (eg. potentially more than 250 individuals concerned) a risk assessment should always be undertaken and properly documented (even if a DPIA is not legally required by the GDPR, in order to comply with Article 32 GDPR).

**2. Contract with the CSP**

**2.1. Briefly describe the issue (s0 identified.**

- Precise definition of the roles of the concerned parties.
- Applicable Law and court seat.
- Question how to ensure CSP acts only on behalf of and according to the documented instructions.

**2.2. Which provision(s) of the GDPR does this concern?**

- Art. 4 GDPR

**2.3. Explain why this has been an issue for your stakeholders?**

- Questions of liability.

**2.4. What are differences that you have encountered between stakeholders in your Member State?**

- -

**2.5. What are solutions to this issue? Please describe if these solutions are already implemented or potential, and whether this solution is provided by the SA or the stakeholders.**

- The Controller has been advised to evaluate regularly whether agreement is kept and if necessary renegotiate.

**3. International transfers and access by foreign public authorities**

**3.1. Briefly describe the issue(s) identified.**

- Question of transfer of Personal Data taking place in the context of routine services provision and possible actions taken by controller to ensure the contractual obligations.

**3.2. Which provision(s) of the GDPR does this concern?**

- Chapter V GDPR, Art. 45 GDPR

**3.3. Explain why this has been an issue for your stakeholders?**

- Destination may fail to ensure essential protection. Controller had to contractually implement appropriate supplementary measures but follow-up assessments have not been conducted yet..

**3.4. What are differences that you have encountered between stakeholders in your Member State?**

- -

**3.5. What are the solutions to these issues? Please describe if these solutions are already implemented or potential, and whether this solution is provided by the SA or the stakeholders.**

- Even though follow-up assessments were deemed necessary, there were no actions or only little. The Controller has been advised to evaluate regularly.

**4. Telemetry data**

**4.1. Briefly describe the issue(s) identified.**

- Because of the applied hybrid operation, user content is processed locally and is not shared with the cloud/third countries.

**4.2. Which provision(s) of the GDPR does this concern?**

- Chapter II and V

**4.3. Explain why this has been an issue for your stakeholders?**

- Even though data protection risks with telemetry data were already public knowledge, stakeholders awareness during the pre-contractual phase was low. Stakeholders had only little to no precise knowledge about the processing, at first.

**4.4. What are differences that you have encountered between stakeholders in your Member State?**

- -

**4.5. What are solutions to this issue? Please describe if these solutions are already implemented or potential, and whether this solution is provided by the SA or the stakeholders.**

- Stakeholder has been advised to report follow-up assessments and measures taken.

**5. Compliance**

**5.1. Briefly describe the issue(s) identified.**

- Even though follow-up assessments were deemed necessary, there were no actions or only little. The Controller has been advised to evaluate regularly.

**5.2. Which provision(s) of the GDPR does this concern?**

- Art. 45 GDPR

**5.3. Explain why this has been an issue for your stakeholders?**

**5.4. What are differences that you have encountered between stakeholders in your Member State?**

**5.5. What are solutions to this issue? Please describe if these solutions are already implemented or potential, and whether this solution is provided by the SA or the stakeholders.**

### **Part III – Actions by the SA**

1. **Have you taken action (i.e. fact finding exercises, informal contact, prior consultation, investigation) towards any of the stakeholders concerning the use of cloud based services prior to launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**
  - Stakeholder has been advised to report follow-up assessments and measures taken.
2. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (e.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

### **Part IV – Other**

1. **What is your general impression of the levels of awareness and compliance of the stakeholders you consulted concerning the use of cloud?**
  - During the pre-contractual-phase awareness was actually quite high, seeing as numerous bodies (internal and external) were consulted beforehand. Follow-up measures have been advised.
2. **Are there any other issues or topics that you would like to flag?**
3. **Are there any best practices that you would like to share?**

# BE SA

(Autorité de protection des données – Gegevensbeschermingsautoriteit)

## Part I – Statistics

### 4. How many stakeholders have you contacted within the following categories?

- Ministry of the central government: The BE SA sent the questionnaire to 1 Ministry of the central government. This Ministry has the specificity of also being a member of the non-profit organisation (see below, under “other”) that provides a community cloud. This set up has an impact on the answers provided by the Ministry.
  - Independent public body of the central government: 1
  - Buyer for the central government
  - Publicly owned company acting as a processor for several central public bodies
  - Ministry of the regional government: 5
  - Independent public body of the regional government
  - Buyer for the regional government
  - Publicly owned company acting as a processor for several regional public bodies
  - Other, please specify: **1 non-profit organisation (publicly owned) that acts as an independent internal ICT service provider for public bodies. This entity acts as a processor for the public bodies and also provides a community cloud.**
- In total, the BE SA sent the questionnaire to 8 stakeholders.

### 5. How many stakeholders have you contacted within the following sectors?

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government: **2**
- Economic affairs
- Education
- Finance
- Health: **1**
- Infrastructure
- Employment
- Justice
- Tax
- Other, please specify: **5 “regional” or “community” bodies that have competencies in the fields of health, education, etc.**

### 6. If you have contacted a buyer, for which sectors does this buyer provides its services:

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government
- Economic affairs
- Education
- Finance
- Health
- Infrastructure
- Employment
- Justice

- Tax
- No specific sector
- Other, please specify: **The BE contacted an independent internal ICT service provider for public bodies (the non-profit mentioned above) but the BE SA did not ask for which sector the latter provides its services as this question was not included in the original questionnaire, so the BE SA does not have this information.**

**7. If you have contacted a buyer, and if you have this information, please specify the number of stakeholders this buyer provides services for:**

- The BE SA remained faithful to the original questionnaire so does not have this information.

**8. What was the initial procedural framework of your action?**

- Fact finding
- Fact finding + determining follow-up action based on the results
- New investigation<sup>1</sup>
- Ongoing investigation
- The initial procedural framework of the action was a fact-finding mission. The objective was to obtain a helicopter view of the use of cloud-based services by public bodies. It was decided that the possible follow-up action(s) would be determined on the basis of the answers to the questionnaire.

**9. How many stakeholders indicated that they use CSPs or are planning to do so in the near future (end of 2022)?**

- 6 out of 8 stakeholders confirmed that they currently use CSPs.

**10. Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?**

- Internal organisation (office suites, internal communication, HR, etc.)
- Exercise of public functions (services to citizens, processing citizen's data, etc.)
- The BE SA asked the respondents to answer the questionnaire only in relation to the most important CSPs used for large-scale processing of personal data of citizens. The BE SA decided not to focus its attention on the use of CSPs for internal organisation purposes, but only in relation to the public bodies' "core" functions/activities.
- Therefore, the BE SA cannot provide a response to this question, given that the BE SA does not have an overview of the use of CSPs for internal organisation purposes.

**11. For the following commonly identified sectors, please specify if any hyper-scalers<sup>2</sup> are involved (if so please name them) either because they provide the services themselves or because the services are using the infrastructures of these hyper-scalers**

- Health
- Finance
- Tax
- Education

---

<sup>1</sup> making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred

<sup>2</sup> Hyper-scalers provide cloud services at scale. It refers usually to the big cloud providers (Google, AWS, Microsoft ...) on which other services may also depend

- Central buyers or providers of IT services
- The following hyper-scalers were mentioned in the questionnaires: AWS, Microsoft.

**12. How many stakeholders took the following actions prior to- or during the acquisition of a CSP?**

- *Perform a DPIA: 2 out of 6 stakeholders.*
- *Does the DPIA analyse transfers in details (sometimes called DTIA): the BE SA does not have this information, as the DPIAs were not communicated by the stakeholders.*
- *Contact the DPO for advice: 3 out of 6 stakeholders.*
- *Perform a general risk analysis: the BE SA does not have this information, as this specific question was not included in the questionnaire.*
- *Contact the SA for advice: this question was not included in the questionnaire but to our knowledge, the BE SA was not consulted by the stakeholders.*

**13. How many stakeholders (including buyers) take the following actions during the use of the CSP?**

- Monitoring technical and organisational measures to ensure compliance: **3 out of 6 stakeholders monitor technical and organisational measures.**
- In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g. Schrems II): **2 out of 6 stakeholders responded that transfers take place. If transfers take place, technical and organisational measures have been adopted by the stakeholders. Sometimes the technical and organisational measures were not specifically described by the stakeholders.** **1 stakeholder (out of 2) claimed that it monitors changes in the regulatory landscape.**
- Regular risk assessments: **2 out of 6 stakeholders responded that they make regular data protection risk assessments. 1 out of 6 stakeholders responded that they make regular data protection risk assessments but without providing clear answers as to the process so the BE SA is not certain that such assessments take place in practice.**

## Part II – Substantive issues

**1. The DPO was not consulted**

- In some cases, the DPO was not consulted prior to selecting and acquiring the services of the CSP.
- However, article 39(1) of the GDPR clearly stipulates that:
- The data protection officer shall have at least the following tasks:

*"(a) to **inform and advise** the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;*

*(b) to **monitor compliance** with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;*

*(c) to **provide advice** where requested as regards the **data protection impact assessment** and monitor its performance pursuant to Article 35;*

(...)".

- One stakeholder did not consult its own DPO as it provides the community cloud and acts as a processor. This does not seem to be a valid argument as Article 37 of the GDPR applies to both controllers and processors with respect to the designation of a DPO and the tasks of the DPO listed on Article 39 of the GDPR applies to processor and controller DPOs.
- One stakeholder did not consult its own DPO, as it is a member of the said non-profit. However, this does not, in our opinion, constitute valid reasons not to consult the DPO in the context of the use of cloud services.
- In addition, one stakeholder did not consult its DPO because it acquired the cloud services through a central regional buyer. Again, this does not, in our opinion, constitute a valid motive not to involve the DPO of the controller.
- Three stakeholders consulted the DPO and sought an opinion. One of these stakeholders detailed that the DPO was involved at different stages of the acquisition of the cloud services, i.e. when preparing the tender documents and throughout the selection process.
- As indicated in the Guidelines on Data Protection Officers ('DPOs'), the GDPR recognises the DPO as a "key player in the new data governance system"<sup>3</sup>.
- In some cases, it appears that the DPO has been side-lined entirely and is not granted this key position in important decisions that involve data protection issues.

## 2. **Carrying out a DPIA**

- A number of the stakeholders did not carry out a data protection impact assessment before selecting and using the services of the CSPs.
- The reasons provided for not carrying out a DPIA are not always based on legal arguments, for example, that the processing carried out in the context of the use of cloud services does not meet the conditions either listed in Article 35(3) of the GDPR or in the list established by the SA.
- One stakeholder did not carry out a DPIA as it does not act as a controller but supports the controllers it provides the community cloud to when they are carrying out a DPIA.
- One stakeholder considers that it must not carry out a DPIA due to the fact that it is a member of the non-profit providing the community cloud. This does not seem like a valid argument.
- One stakeholder confirms that various DPIAs have been performed, but it is not clear if the DPIAs also address the processing carried out in the context of the use of cloud services.
- One stakeholder affirms that it intends to use the DPIA carried out and made public by the Nederlandse Rijksoverheid entitled "Public DPIA Team OneDrive Sharepoint and Azure". The stakeholder intends to analyse the scope of the DPIA and shall make an additional DPIA concerning its use of CSPs if needed. The analysis is ongoing, despite the fact that the cloud services have been in use for some time. However, Article 35(1) of the GDPR clearly stipulates that a DPIA must be carried out prior to the processing. In addition, a DPIA must take account of the nature, scope, context and purposes of the specific processing envisaged. The stakeholder

---

<sup>3</sup> Guidelines on Data Protection Officers ('DPOs') of the Art. 29 Data Protection Working Party, p. 5.

must therefore carry out its own DPIA that relates specifically to the processing done by the CSP on its request.

- The DPIA, which constitutes an important tool for accountability, is a “*process for building and demonstrating compliance*”<sup>4</sup>. This does not seem to be understood by several of the stakeholders.
- Stakeholders must understand that the DPIA has to be carried out before the processing starts and also that they must carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations (article 35(11) of the GDPR).

### **3. Data protection requirements in the public procurement documents**

- Article 28(1) of the GDPR stipulates that “*Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject*”.
- Despite this obligation, several of the public bodies did not include detailed data protection requirements or certification requirements in the tender/public procurement documents. This seems to indicate that the obligation to “only use processors providing sufficient guarantees” is not fulfilled as data protection requirements are not taken into account when choosing the CSPs.
- In one case, the stakeholder argued that this was due to the fact that it went through a central regional buyer to acquire the CSP and so had no control over the tender process or the requirements included in the documents. The stakeholder argues it does not have the means to organise tenders.
- Another stakeholder, that benefited from a European framework agreement to use the cloud services, affirmed that information security requirements were included in the tender (including ISO 270001 certification).
- Yet another stakeholder included detailed requirements in relation to data protection in its tender documents: confidentiality, technical and organisation measures, restriction of transfers to third parties, rights of the data subjects, deletion or return of the data at the end of the contract, etc.).
- Including such requirements in the public procurement seems to be essential to ensure that only processors complying with data protection requirements and therefore meeting the conditions set out in Article 28 of the GDPR are selected by the controllers.

### **4. Contract between the controller and the CSP**

- Two stakeholders had not yet signed a contract pursuant to Article 28(3) of the GDPR with the CSP, even though the processing is already ongoing.
- This is problematic as Article 28(3) of the GDPR clearly stipulates that the processing by the processor shall be governed by a contract or other legal act under Union or Member State law that is binding on the processor with regard to the controller.

---

<sup>4</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 of the Art. 29 Data Protection Working Party, p.4.

- Some stakeholders indicated that the CSPs standard contract had to be concluded in order to use the services and there was no possibility to negotiate a bespoke contract. This may be problematic in relation to the content of the contract and its conformity with article 28(3) of the GDPR, leaving no margin of negotiation for the controller and therefore possibly not enabling the controller to remain in control of the personal data.
- The controllers should make sure that such contracts are signed before the start of the processing and that they contain all the requirements if Article 28(3) of the GDPR.
- The standard contracts signed by some of the stakeholders contained general authorisation to use sub-processors, as allowed by Article 28(2) of the GDPR: "*The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall 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*". The question of whether the controller is offered a meaningful opportunity to object to changes of sub-processors is raised.

##### **5. International transfers**

- In one case, the stakeholder seemed to provide contradictory information in relation to the possible transfers to third countries, which indicates that the controller does not always have a clear picture of the data transfers operated by the CSPs in the context of the execution of the contract.
- In another case, the stakeholder responded that transfers take place only to one country with an adequacy decision. However, in the standard contract of the CSP the stakeholder refers to, it is clearly stipulated that the data will be processed only in the locations specified by the customer, "*except as necessary to provide the Services initiated by the Customer or as necessary to comply with the law or binding order of a governmental body*".
- It appears that some stakeholders have limited knowledge of whether third country transfers take place.
- Several stakeholders did not check, in light of the Schrems II judgement, that there is nothing in the third country's legislation and/or practices that prohibits the recipients from complying with their contractual obligations in order to ensure that the level of data protection of natural persons guaranteed in the EEA is not undermined.
- The stakeholders should ensure that they have precise information on the actual transfers of personal data to third countries that take place and that the processors they select respect the provisions of Chapter V of the GDPR and the Schrems II ruling.

### **Part III – Actions by the SA**

1. **Have you taken action (i.e. fact-finding exercises, informal contact, prior consultation, investigation) towards any of the stakeholders concerning the use of cloud-based services prior to launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the stakeholder, general guidance,**

**corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

- No, the BE SA did not launch any action prior to launching the coordinated action.
2. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (E.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**
- The BE SA waited for the outcome of the discussions within the CEF in order not to compromise any of the work done within the working group. The BE intends to send letters to the stakeholders to which the questionnaires were sent. The objective is to enable the stakeholders to make a self-assessment and take the necessary measures to comply with their data protection obligations and possibly also renegotiate the terms with the CSPs.

#### **Part IV – Other**

1. **What is your general impression of the levels of awareness and compliance of the stakeholders you consulted concerning the use of cloud?**
- The BE SA's general impression is that there are big disparities in the level of awareness and compliance of the stakeholders.
  - 1 stakeholder had a very high level of compliance/awareness. 4 stakeholders had medium to high level of compliance and 1 stakeholder had very low levels of compliance/awareness.
  - In some cases, this was partially explained by the fact that the stakeholder had acquired the CSP's services through a central buyer. Consequently, there was some misperception on the allocation of responsibilities (consulting its own DPO, carrying out a DPIA, etc.) but also little to no control over the public procurement process.
2. **Are there any other issues or topics that you would like to flag?**
- No.
3. **Are there any leading practices of the stakeholders you have contacted that you would like to share?**
- No.

## Part I – Statistics

**1. How many stakeholders have you contacted within the following categories?**

- We have contacted the Deputy Ministry of Research, Innovation and Digital Policy (DMRIDP), which acts as the buyer for the central government as regards to cloud services.

**2. How many stakeholders have you contacted within the following sectors?**

- Digitalisation of the Public Administration/e-Government (DMRIDP as mentioned above)

**3. If you have contacted a buyer, for which sectors does this buyer provides its services:**

- Digitalisation of the Public Administration/e-Government

**4. If you have contacted a buyer, and if you have this information, please specify the number of stakeholders this buyer provides services for:**

- All public bodies under the Central Government.

**5. What was the initial procedural framework of your action?**

- Fact finding + determining follow-up action based on the results

**6. How many stakeholders indicated that they use CSPs or are planning to do so in the near future (end of 2022)?**

- 1 (DMRIDP)

**7. Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?**

- Internal organisation (office suites, internal communication, HR, etc.)

**8. For the following commonly identified sectors, please specify if any hyper-scalers<sup>5</sup> are involved (if so please name them) either because they provide the services themselves or because the services are using the infrastructures of these hyper-scalers**

- Central buyers or providers of IT services (Microsoft)

**9. How many stakeholders took the following actions prior to- or during the acquisition of a CSP?**

- Perform a DPIA: **1 DMRDP**
- Does the DPIA analyse transfers in details (sometimes called DTIA): **1 (DMRIDP) (although not in detail)**
- Contact the DPO for advice
- Perform a general risk analysis: **1 (DMRIDP)**
- Contact the SA for advice: **1 (DMRIDP)**

**10. How many stakeholders (including buyers) take the following actions during the use of the CSP?**

- Monitoring technical and organisational measures to ensure compliance: **1 (DMRIDP)**

---

<sup>5</sup> Hyper-scalers provide cloud services at scale. It refers usually to the big cloud providers (Google, AWS, Microsoft ...) on which other services may also depend

- In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g. Schrems II): **1 (DMRIDP)**
- Regular risk assessments: 1 (DMRIDP)

## Part II – Substantive issues

- The DMRIDP, as mentioned on their answers from the questionnaire, has already proceeded with the purchase of 1500 licences of Microsoft Office 365 and is planning to sign an Enterprise Agreement for online cloud products such as Microsoft Teams, OneDrive and SharePoint. Moreover, after studying the DPIA and further responses to our questions, our SA has identified the following issues connected with this purchase

### **1. Issue 1**

- The DMRIDP cannot guarantee that the use of the Microsoft's cloud service is compliant with the Schrems II ruling. There is a high data protection risk related to the possible access by US law enforcement and national security services to personal data and special categories of personal data. This risk occurs even though Microsoft Teams, OneDrive and SharePoint content data are exclusively processed and stored in the EU. Access to data on the EU located servers can be also ordered through US legislation such as the US CLOUD Act.
- As mentioned in the DPIA, this high risk can be mitigated for OneDrive and SharePoint by using their own encryption keys, with Microsoft Double Key Encryption. Microsoft does not yet offer end-to-end encryption for the streaming communication with multiple participants in Teams, only for unscheduled one-to-one video calls. Though Microsoft has confirmed that it will support E2EE in Teams group meetings and chat, it does not yet provide a deadline.
- For non-sensitive categories of personal data, the transfer risks are assessed as very low according to the DPIA, even though the possible impact on data subjects can be very high. The chance that Microsoft is compelled to disclose personal data from EU public sector customers is very slim. Though Microsoft cannot disclose if it has received any specific legal demands subject to a secrecy obligation. Microsoft publicly explains: "Microsoft does not provide, and has never provided, EU public sector customer's personal data to any government." This historical fact, combined with the use of the encryption applied by Microsoft, its legal guarantees of contesting each order, its proven track record and its transparency reports, may be sufficient to qualify the risk of undue access to the 'regular' personal data as a low data protection risk.

### **2. Issue 2:**

- Microsoft shares data with third parties acting as sub-processors to support functions such as customer and technical support, service maintenance, and other operations. In such cases, there is a risk of losing the control of the relevant data. Additionally, it is difficult to monitor the level of protection applied by the sub-processors, thus the DMRIDP as the controller, will not be able to prove compliance with Articles 24 and 28 GDPR.
- In the DPIA it is mentioned that any subcontractors to which Microsoft transfers Support and Consulting Data will have entered into written agreements with Microsoft that are no less protective than the data protection terms of the MPSDPA. All third-party sub-processors with which Support and Consulting Data is shared under the MPSDPA are included in the Microsoft Commercial Support Contractors List.

- Microsoft will not disclose Support and Consulting Data to US authorities unless required by law. If US authorities contact Microsoft with a demand for Support and Consulting Data, Microsoft will attempt to redirect the law enforcement agency to request the data directly from the customer. If compelled to disclose Support and Consulting Data to law enforcement, Microsoft will promptly notify the customer and provide a copy of the demand unless legally prohibited from doing so.
- Upon receipt of any other third-party request for Support and Consulting Data, Microsoft will promptly notify the customer unless prohibited by law. Microsoft will reject the request unless required by law to comply. If the request is valid, Microsoft will attempt to redirect the third party to request the data directly from the customer.

### **3. Issue 3:**

- Transfer of telemetry/diagnostic data to the US. Diagnostic data is used to keep Office secure and up-to-date, detect, diagnose and remediate problems, and also make product improvements.
- According to Microsoft, this data does not include a user's name or email address, the content of the user's files, or information about apps unrelated to Office. This diagnostic data is collected and sent to Microsoft about Office client software running on the user's device in the client organization.
- There are three levels of diagnostic data for Microsoft 365 Apps for enterprise client software:
  - Required: The minimum data necessary to help keep Office secure, up-to-date, and performing as expected on the device it is installed on.
  - Optional: Additional data that helps to make product improvements and provides enhanced information to help detect, diagnose, and remediate issues.
  - Neither: No diagnostic data about Office client software running on the user's device is collected and sent to Microsoft. However, it is not clear whether this option differentiates from the above option "Required" as regards to the data collected.
- Microsoft has not provided an exact description of what data is collected and sent to the US for diagnostic purposes. Additionally, there does not seem to be a way to turn off Office telemetry completely.
- The DMRID, through their own investigation found that, though Microsoft will still transfer some personal data to the USA, to detect and solve security incidents, these ongoing transfers will be incidental, not structural, and they will generally only involve pseudonymised and aggregated data, thus minimizing the risks involved.

## **Part III – Actions by the SA**

1. **Have you taken action (i.e. fact-finding exercises, informal contact, prior consultation, investigation) towards any of the stakeholders concerning the use of cloud-based services prior to launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**
  - The DMRID has shared with our SA the strategy regarding the general use of cloud services by the central government, specifically the development of a hybrid private government cloud for use

by all public authorities. Following this, and a proposed DPIA received regarding the registration of elementary student using a cloud storage service, the Commissioner deemed it necessary, in carrying out her duties under the General Data Protection Regulation (EU) 2016/679, in compliance with the provisions of Article 57(1) (c), to inform the DMRIDP fully about all aspects and parameters relating to the provision of cloud computing services and in particular with regard to the risks that these services may entail. It was also pointed out that in the case of public authorities, which collect and process citizens' personal data on the basis of their legal obligations or in the exercise of the public authority granted to them, citizens, as data subjects, do not have reasonable expectation that their data collected by a public authority is transmitted and hosted in data centres of the provider or its partners in various third countries. This rationale makes even greater the obligation of the public authorities to take every possible action for ensuring the proper transparency of the process, by properly informing the data subjects, in compliance with the provisions of Articles 13 and 14 as the case may be.

2. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (E.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**
  - Currently, our SA plans to continue issuing recommendations to the DMRIDP and ensure that no CSPs are obtained without taking the appropriate remedies for the risks identified. Moreover, in the case of non-compliance or cooperation by the DMRIDP or any public body using CSPs, the Commissioner will also consider using corrective measures if necessary. Our SA will also take into consideration the results of the coordinated action as well as any developments regarding the new USA adequacy decision under discussion.

#### **Part IV – Other**

1. **What is your general impression of the levels of awareness and compliance of the stakeholders you consulted concerning the use of cloud?**
  - Overall, we believe that the DMRIDP was fully aware of the risks involved when purchased the licenses for the use of Microsoft 365 tools (Teams, OneDrive, and SharePoint). While we acknowledge that the integration of such tools is important for the digitalization of services offered to the public, we remain concerned, that in the absence of an adequacy decision, the transfer of data to the US and/or third countries' subcontractors and/or the US Authorities potential access to data stored in the EU, relies on standard contractual clauses, for which third parties such as the DMRIDP have little or no power of control.
2. **Are there any other issues or topics that you would like to flag?**
3. **Are there any leading practices of the stakeholders you have contacted that you would like to share?**

In needs to be stated, that the onsite inspection is still ongoing to the date of submission of this National Report. All the preliminary findings stated bellow are still subject to the examination.

### Part I – Statistics

**1. How many stakeholders have you contacted within the following categories?**

- Ministry of the central government: 2
- Independent public body of the central government: 1 (NOTE: The National Agency for Communication and Information Technologies is a state-owned company established in accordance with Act No. 77/1997 Coll., On State Enterprises, the founder is the Ministry of the Interior. It is a legal entity carrying out business activities with state property in its own name and under its own responsibility. However, it is not independent public body of the central government.)

**2. How many stakeholders have you contacted within the following sectors?**

- Digitalisation of the Public Administration/e-Government: 1 – **National Agency for Communication and Information Technologies (NAKIT)**
- Economic affairs
- Education
- Finance
- Health
- Infrastructure
- Employment: 1 – **Ministry of Labour and Social Affairs (MoLSA)**
- Justice
- Tax
- Other, please specify: **Internal affairs: 1 – Ministry of Interior (Mol)**

**3. If you have contacted a buyer, for which sectors does this buyer provides its services:**

- Not applicable

**4. If you have contacted a buyer, and if you have this information, please specify the number of stakeholders this buyer provides services for:**

- Not applicable

**5. What was the initial procedural framework of your action?**

- Fact finding + determining follow-up action based on the results

**6. How many stakeholders indicated that they use CSPs or are planning to do so in the near future (end of 2022)?**

- All stakeholders currently use CSPs.
- Two stakeholders (NAKIT and Mol) identified one (the same) cloud-based service that processes personal data, The Citizen's Portal. Mol is the controller while NAKIT is the processor. Neither NAKIT nor Mol indicated any use of CSPs in another instance. (NOTE: The answers to all of the following questions apply only to NAKIT and Mol and all of the answers apply to The Citizen's Portal. Since the CSP is used to run The Citizen's Portal, all the answers are given on behalf of Mol as the controller while NAKIT as the processor is regarded as NOT using CSP at all)

- One stakeholder (MoLSA) claims not to use them for such processing. 1 stakeholder (NAKIT) claims not to use CSPs at all (other than CSP used to run the Citizen's Portal).

**7. Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?**

- Internal organisation (office suites, internal communication, HR, etc.)
- Exercise of public functions (services to citizens, processing citizen's data, etc.): **1**

**8. For the following commonly identified sectors, please specify if any hyperscalers are involved (if so please name them) either because they provide the services themselves or because the services are using the infrastructures of these hyper-scalers**

- Central buyers or providers of IT services: **1** stakeholder utilizes Microsoft Azure.

**9. How many stakeholders took the following actions prior to- or during the acquisition of a CSP?**

- Perform a DPIA: **1**
- Does the DPIA analyse transfers in details (sometimes called DTIA): **No**
- Contact the DPO for advice: **1**
- Perform a general risk analysis: **1**
- Contact the SA for advice: **0**

**10. How many stakeholders (including buyers) take the following actions during the use of the CSP?**

- Monitoring technical and organisational measures to ensure compliance: **1**
- In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g. Schrems II): **Data centres are in the EU, no transfer takes place.**
- Regular risk assessments: **1**

## Part II – Substantive issues

### 1. DPIA

- Preliminary findings suggest that the DPIA has not been thoroughly done accordingly to the items set out in Art. 35(7) GDPR. MoI is of the opinion that a DPIA is not a mandatory document in this case.
- Art. 35 GDPR, Article 10 of Act No. 110/2019 Coll., On Personal Data Processing.
- Preliminary findings suggest that the DPIA does not reflect whether alternatives (other than a cloud-based service) were considered. Moreover, the DPIA does not contain any assessments as required by Art. 35(7) (b/c) GDPR.
- Requirements laid down in Art. 35(7) (d) GDPR appear not to be met – the DPIA lists the measures taken, but they are not assigned to the risks. It is not clear, what specific measures were taken to mitigate a particular risk.
- Preliminary findings have revealed that the DPO of the controller was not involved in the manner prescribed by Art. 35(2) GDPR.
- Furthermore, the controller is of the opinion that any DPIA is not needed at all pursuant to Article 10 of Act No. 110/2019 Coll., On Personal Data Processing. This section of the national law states that a controller is not obliged to carry out DPIA in the situation where it is stated by law that the controller has to carry out a specific processing operation. The CZ SA has opposed to such interpretation of the national law, as it was not interpreted in accordance with the GDPR.
- Not applicable

- If the preliminary findings are upheld, the CZ SA will insist that the controller takes measures to amend the DPIA. The controller will be approached due to the differing opinions on whether the DPIA is obligatory.

## **2. Contract pursuant to Art. 28 GDPR**

- Preliminary findings suggest that only a general contract between the controller (Mol) and the processor (NAKIT) has been concluded.
- Art. 28 GDPR, mainly Art. 28 (3) GDPR.
- Preliminary findings indicate, that there is only a general contract between the controller (Mol) and the processor (NAKIT) (it needs to be noted that there are two more sub-processors, T-Mobile Czech Republic a.s. and MICROSOFT s.r.o. at the end) that serves as a basis for a range of services provided by the processor to the controller, whereas only one of them is The Citizen's Portal. This appears to constitute a breach of Art. 28 (3) GDPR that stipulates, that a contract shall set out "the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects", since none of the cited is specified in the contract in relation to The Citizen's Portal.
- Not applicable
- The controller will be obliged (in case the above stated findings have been confirmed) by the CZ SA to amend the contract so it is specific as per requirements set out in Art. 28 (3) GDPR.

## **3. Use of Microsoft Azure**

- The Mol declared the use of Microsoft Azure as their cloud platform.
- Articles 44-49 GDPR may be concerned.
- In light of the Schrems II judgment, it is not clear whether the use of such services involves the transfer of personal data (e.g. IP addresses) to the United States of America.
- Not applicable
- According to the Mol, contracts with providers were set up so that all data processed under the use of cloud services were stored exclusively in data centres geographically located in the EU. Further investigation will show whether this condition has been met. It will also be necessary to decide whether such conditions are sufficient in the light of Schrems II.

## **Part III – Actions by the SA**

1. Have you taken action (i.e. fact-finding exercises, informal contact, prior consultation, investigation) towards any of the stakeholders concerning the use of cloud-based services prior to launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).
  - Only a general communication on principles regarding transfers of personal data to 3rd countries took place.
2. What action(s) are you planning to undertake based on the results of this coordinated action, if any? (E.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)

- An on-site inspection is currently under way. Based on the facts established, consideration will then be given to the possible further use of the investigative and corrective powers vested in the CZ SA.

#### **Part IV – Other**

**1. What is your general impression of the levels of awareness and compliance of the stakeholders you consulted concerning the use of cloud?**

- It can be stated that a potentially problematic issue of personal data transfer to 3rd countries has been identified, however, it is clear from the stakeholder's statements that they are at least aware of these risks and try to mitigate them in certain ways, such as using data centres in the EU. Furthermore, it is the impression of the CZ SA that while focus (rightfully so) of the controller is given to the obligations under Art. 25 and 32, other obligations under the GDPR are neglected, mainly those related to Art. 28 and 35 GDPR.

**2. Are there any other issues or topics that you would like to flag?**

- Not applicable

**3. Are there any leading practices of the stakeholders you have contacted that you would like to share?**

- Not applicable

# DE SA

## Part I – Statistics

### 1. How many stakeholders have you contacted within the following categories?

- Ministry of the central government
- Independent public body of the central government
- Buyer for the central government
- Publicly-owned company acting as a processor for several central public bodies: **1**
- Ministry of the regional government: **1**
- Independent public body of the regional government
- Buyer for the regional government
- Publicly-owned company acting as a processor for several regional public bodies
- Other, please specify: **8 (categories: health insurance, processor for health insurance, pension insurance, labour administration, central it service provider)**

### 2. How many stakeholders have you contacted within the following sectors?

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government: **2**
- Economic affairs
- Education
- Finance
- Health: **6**
- Infrastructure
- Employment: **1**
- Justice
- Tax
- Other, please specify: **1 pension insurance**

### 3. If you have contacted a buyer, for which sectors does this buyer provides its services:

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government
- Economic affairs
- Education
- Finance
- Health
- Infrastructure
- Employment
- Justice
- Tax
- No specific sector: **2**
- Other, please specify: **IT service provider for the federal public sector**

### 4. If you have contacted a buyer, and if you have this information, please specify the number of stakeholders this buyer provides services for:

- Information not provided.

### 5. What was the initial procedural framework of your action?

- Fact finding: **X**
  - Fact finding + determining follow-up action based on the results
  - New investigation
  - Ongoing investigation
- 6. How many stakeholders indicated that they use CSPs or are planning to do so in the near future (end of 2022)?**
- 9
- 7. Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?**
- Internal organisation (office suites, internal communication, HR, etc.): **8**
  - Exercise of public functions (services to citizens, processing citizen's data, etc.): **up to 4**
- 8. For the following commonly identified sectors, please specify if any hyper-scalers are involved (if so please name them) either because they provide the services themselves or because the services are using the infrastructures of these hyper-scalers**
- Health: **5**
  - Finance
  - Tax
  - Education
  - Central buyers or providers of IT services: **3**
  - pension insurance: **1**
- 9. How many stakeholders took the following actions prior to- or during the acquisition of a CSP?**
- Perform a DPIA: **3**
  - Does the DPIA analyse transfers in details (sometimes called DTIA): **2**
  - Contact the DPO for advice: **3**
  - Perform a general risk analysis: **6**
  - Contact the SA for advice: **1**
- 10. How many stakeholders (including buyers) take the following actions during the use of the CSP?**
- Monitoring technical and organisational measures to ensure compliance:
  - In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g. Schrems II): **4**
  - Regular risk assessments: **7**

## Part II – Substantive Issues

### Preliminary note

The DE SAs investigated a total of 10 public entities at federal and regional level. As the individual projects examined differ greatly from one another the following report is divided in parts and sections. Each part/section is dedicated to one or more DE public institutions. The first part deals with stakeholders actually using cloud service, while the second part examines a proof of concept concerning the use of an intermediate encryption service.

### Part II.1. Stakeholders actually using cloud services

General remarks on the subject of questions I., 2. g) -j) (personal data):

A) 1. In the case of identical task areas, an allocation of data processing processes, in particular to the higher level of protection according to Art. 9 GDPR (above all health data) by the supervised bodies is inconsistent.

Applications from CSPs are used by public bodies for identical areas of responsibility. The statements of the supervised bodies differ as to whether the data processing concerns core areas of the fulfilment of tasks and whether this at least also involves health data, which are subject to the higher level of protection under Art. 9 GDPR.

2. Relevant regulations:

- a. Art. 5 GDPR
- b. Art. 6 GDPR
- c. Art. 9 GDPR
- d. Art. 4 GDPR
- e. Art. 28 GDPR
- f. Art. 32 GDPR
- g. sec. 35 para. 2 of the German Social Code (SGB) Book I, sec. 67 ff. of the German Social Code Book X

The questions mentioned under point 1 have a direct effect on the assessment of the lawfulness of the data processing - especially in the area of Art. 9 GDPR. The question of whether health data are processed by the CSP determines the opening of the scope of protection of Art. 9 GDPR. The question of whether health data are processed for the core area of task fulfilment primarily leads to legal reviews under Art. 32(2) of the GDPR and Section 80(2) of the German Social Code Book X. If health data are processed by the CSP outside the core area of task fulfilment, it must be examined whether the legal grounds for permission apply or whether explicit consent is required according to Art. 9 para. 2 lit. a) GDPR. In the latter case, in addition to the challenge of an informed decision, the aspect of "voluntariness" is also problematic due to the subordination relationship.

Due to the broad variance in descriptions, the data processing by the CSP could also first be reviewed on the basis of the data minimisation principle.

The common interest is to be able to guarantee the fulfilment of tasks and to have legally compliant and suitable data processing means available on the market for this purpose and to be able to use them in a data protection compliant manner. First, a uniform terminological understanding of data protection must be created and the corresponding data processing procedures must be reflected transparently.

B) Regarding one central IT service provider no substantial issues have been identified from the information provided. However, the report did not seem to be complete and an improved version has not been delivered in time, although a revised document was requested.

The only productive cloud service described is cloud hosted by the service provider itself, providing various IaaS, PaaS, and SaaS services for public authorities.

The supervisory authorities have been involved as consultant from an early phase. The service provider only acts as processor, controllers are assisted with DPOs, if necessary. As no actions were planned, contracts have not been requested with the questionnaire therefore no assessment can be made.

The self-hosted cloud is only operated in the service provider's data centres located in Germany and services are only provided to German public bodies. No data transfers to third countries occur. Diagnostic data is collected according to the BSI Act, which provides the legal basis for possible measures in this field

Implementation of technical and organizational matters as well as compliance with the data protection concept is ensured via regular audits by the supervisory authority.

C.) 1. Personal data (communication data) is collected via registration and in the context of participation in the virtual event. Special categories of personal data or social data are not processed. An increased need for protection is not apparent. The transmission of telemetry data is prevented as far as possible. The processing of additional telemetry data generated in the cloud cannot be ruled out according to current knowledge.

2. Relevant regulations:

- a. Art. 5 GDPR
- b. Art. 6 GDPR
- c. Art. 9 GDPR
- d. Art. 4 GDPR
- e. Art. 28 GDPR
- f. Art. 32 GDPR
- g. Sec. 26 of the German Federal Data Protection Act (BDSG)

The questions mentioned under point 1 have a direct effect on the assessment of the lawfulness of the data processing. The question of whether social data is processed for the core area of task fulfilment does not arise here after the feedback, so that a legal review according to Art. 32 para. 2 GDPR and sec. 80 para. 2 of the German Social Code (SGB) Book X is dispensable. Since employee data may also be affected here, the question of effective consent to data processing appears questionable. In addition to the challenge of an informed decision, the aspect of "voluntariness" is also problematic due to the subordination relationship.

The common interest is to be able to guarantee the fulfilment of tasks and to have legally compliant and suitable data processing means available on the market for this purpose and to be able to use them in a data protection compliant manner. First, a uniform terminological understanding of data protection must be created and the corresponding data processing procedures must be reflected transparently.

Thematic sensitisation can take place by means of information campaigns or on the occasion of supervisory measures.

## **Part II.2. Substantive issues**

### **Part II.2.1 Pre-Contract/Procurement Criteria**

- On the topic of "acquisition of cloud services"

1. Relevance and coverage of the data protection challenges/requirements for tenders and award decisions.

All surveys showed that data protection requirements are included in tendering and award procedures. The feedback, however, showed a variance in terms of bindingness or as possible grounds for exclusion. This can subsequently lead to problems, as procurement criteria cannot easily be changed after the award decision.

In some cases, pre-DPIAs, here essentially an analysis of the nine criteria for high-risk processing operations according to WP 248 of the Article 29 data protection working party, were conducted before the procurement to determine necessary data protection requirements.

2. Relevant regulations:

- a. GDPR as a whole
- b. Chapter 2 of the German Social Code (SGB) Book X
- c. European and German public procurement law

3. The public bodies have to fulfil their legal duties. Due to digitisation strategies and economic considerations, processes must be redesigned, for which the market provides limited products. The mandatory data protection requirements are often in conflict with the technical requirements resulting from the legal mandates due to market conditions.

4. In some cases, stakeholders have joined forces in order to achieve a better negotiating position for the enforcement of data protection requirements. However, this approach could not completely eliminate the tension.

5. Data protection requirements must be brought to the attention of the market through supervisory measures but also through socio-political discussions. Furthermore, a joint approach of dealing with the existing discrepancies between the available products and the legal requirements/developments of data protection at the European level would be most welcome (especially against the background of the Schrems II decision of the ECJ).

In the future, "GDPR certifications" could be used as a suitable means for award criteria in IT tendering.

#### **Part II.2.2 International transfer**

On the subject of "Contract and International Transfer"

A) 1. The problem is largely reflected in the widespread use of American applications. There is a transfer of data to third countries. This allows access for foreign governments even in the case of non-EU customer service providers who only offer their services from the EEA. The powers of the US intelligence services are problematic here; due to the legal situation in the USA, an adequate governmental level of data protection (Art. 45 DS-GVO) cannot be ensured. The standard contractual clauses adopted by the Commission in 2010 are no longer sufficient for data transfers to third countries without any additional measures.

2. Relevant regulations:

- a. Art. 5 GDPR
- b. Art. 6 GDPR
- c. Art. 4 GDPR
- d. Art. 28 GDPR
- e. Art. 32 GDPR
- f. sec. 80 para. 3 of the German Social Code (SGB), Book X in conjunction with Art. 45 GDPR
- g. Art. 46 para. 1 GDPR

3. The stakeholder group is the health sector. All public bodies in the health sector that transfer data to the USA, especially if they have previously based the transfer on the Privacy Shield, but also if they used the old standard contractual clauses from 2010 for this purpose, transfer sensitive social and health data to third countries.

It is questionable whether the legitimate interests are safeguarded if a transfer is not made or the consent of the data subject is obtained. In principle, the general interest prevails.

4. Differences in stakeholder groups: There are hardly any transfers to third countries.

- Awareness of third country issues (Schrems II),
- Willingness to introduce further measures exists
- Implementation and further development of technical and organisational measures

5. Action will be taken with all stakeholders and awareness of third country issues will be raised. Contractual and technical restriction of processing to the EU will take place. In addition, further technical measures have been agreed to prevent personal data from leaving the geolocation (Premium Support Contract: Customer Lock Box, Local Support Engineer). Transfers of personal data outside the EU will have to be approved by the client on a case-by-case basis (e.g. for support).

In addition, the processing of personal data is regularly restricted to the EEA in the contracts with CSPs. Special attention will be paid to conclude contracts for the provision of cloud services generally only with CSPs located in the EEA. If, in individual cases, a CSP outside the EEA is appointed, contractual parties shall agree on further safeguards (e.g. in accordance with the requirements of the German and European data protection authorities) in addition to the inclusion of currently valid standard contractual clauses.

Encryption of data according to the "Bring your Own Key" principle and specific additional agreements for social data are planned.

The creation of security concepts is planned.

Further problems exist in the implementation of physical controls in the technical facilities of the third countries ("access controls").

B) 1. The issue is largely reflected in the use of a cloud offering from a third-country provider. Data transfer to third countries cannot be ruled out. This allows access for foreign governments even in the case of the use of non-EU account managers who only offer their services from the EEA. The powers of the US intelligence services are problematic here; due to the legal situation in the USA, an adequate state level of data protection (Art. 45 DS-GVO) cannot be ensured. The standard contractual clauses adopted by the Commission in 2010 are no longer sufficient for data transfers to third countries without additional measures. However, the current, adapted standard contractual clauses are used here.

2. Relevant regulations:

- a. Art. 5 GDPR
- b. Art. 6 GDPR
- c. Art. 4 GDPR
- d. Art. 28 GDPR
- e. Art. 32 GDPR
- f. sec. 80 para. 3 of the German Social Code (SGB), Book X with Art. 45 GDPR
- g. Art. 46 para. 1 GDPR

3. The stakeholder group here is the education sector in the social administration department. It is questionable whether the legitimate interests would be safeguarded if the data were not transferred or if the consent of the data subject were obtained. In principle, the general interest prevails.

4. Differences in the stakeholder groups: Based on the questionnaires, it is clear that hardly any or no transfers take place to third countries. It can be concluded that there is

- Awareness of the third country problem (Schrems II)
- Willingness to introduce further measures - Implementation and further development of technical and organisational measures
- Implementation and further development of technical and organisational measures

5. Measures are being worked on with all stakeholders and awareness of the third-country problem is being raised. The current, adapted standard contractual clauses are used. The validity of German law, the use of European servers and the compliance with contractually agreed technical and organisational measures have been contractually agreed. Further problems exist in the implementation of physical

controls in the technical facilities of the third countries ("access controls"). The possibility of on-site inspections by the contracting authority and the competent legal and technical supervision was contractually agreed.

#### **Part II.2.3 Necessary telemetry data**

On the topic of "diagnostic/telemetry data":

1. Product-specific statements regarding the collection on user computers vs. CSP servers or the use of anonymised, pseudonymised or real data can only be made in general terms. Some diagnostic/telemetry data is considered to be non-personal data, although direct or indirect identification of data subjects cannot be excluded.

2. Relevant regulations:

- a. Art. 5 GDPR
- b. Art. 6 GDPR
- c. Art. 4 GDPR
- d. Art. 28 GDPR
- e. Art. 32 GDPR

3. to 5. Primarily a technical referral is required to analyse the circumstances, assess interests and develop solutions.

#### **Part II.2.4 Monitoring/Compliance**

On the subject of "Contract and International Transfer"

A) 1. The problem lies primarily in the unclear jurisdiction.

The implementation of long-term measures requires a precise definition of these additional measures, which must also be implemented in the next step, i.e. they must also be available effectively and practically. For some health insurance funds, the details for future audits have not yet been determined.

2. Relevant regulations:

- a. Art. 5 GDPR
- b. Art. 6 GDPR
- c. Art. 4 GDPR
- d. Art. 28 GDPR
- e. Art. 32 GDPR
- f. sec. 80 para. 3 of the German Social Code (SGB), Book X with Art. 45 GDPR
- g. Art. 46 para. 1 GDPR

3. Implementation of procedures for dealing with data breaches and notifications pursuant to Articles 33 and 34 GDPR.

- Procedures for dealing with the exercise of the rights of the data subject.

This in turn may require further external monitoring for the health insurance funds. This external accompaniment could constitute a subcontracted processor.

4. Some health insurance funds are already carrying out risk assessments, whereas other health insurance funds must implement measures before doing so.

Details of the audits have not yet been determined; some software producer offer, among other things, that audits will be made (external audit also conceivable);

5. Among other things, group-wide data protection management systems (DSMS) and information management systems (ISMS) have been established at the statutory health insurance funds to ensure compliance with data protection laws and the security of the processing of personal data. Various

group-wide binding guidelines are derived from guidelines on data privacy and information security. Further solutions provide for existing risk analyses and DPIAs are to be reviewed every 2 years at the latest and that monitoring is to be carried out on the basis of the processor contract.

Risk assessments are carried out as part of the preparation and updating of the data protection impact assessment. In accordance with the Supplier Management Policy and "DSM Risk Assessment and the data protection impact assessment", the risk assessment is considered again in the regular service provider review as well as in the regular review of the documents and, if necessary, there is response to new finding.

B. 1. The control of technical and organisational measures is carried out by the responsible department through IT administration, IT security and the data protection unit. In addition, there is a regular exchange and further training. Monitoring of telemetry data is carried out by IT security and system administration in day-to-day business. However, monitoring is geared towards external attacks and irregularities. A procedural notification is available; a data protection impact assessment is still pending and is currently being prepared.)

2. Relevant regulations:

- a. Art. 5 GDPR
- b. Art. 6 GDPR 8
- c. Art. 4 GDPR
- d. Art. 28 GDPR
- e. Art. 32 GDPR

C. One of the responses indicates that monitoring of security measures and information security risk assessments (ex-post) are only carried out if necessary, i.e., only contract adjustments and innovations on the part of the processor are reviewed. And further "*work is underway to establish a process*".

### **Part II.3. Investigation of a Proof of Concept (PoC)**

Object of one investigation was a proof of concept (PoC). The stakeholder can be seen as central buyer in the sense of the CEF providing the contractual setting for different areas government / administration.

The concept of the PoC aims at encrypting data before it is transferred to the cloud by an intermediate encryption component. Background of the PoC is an announcement by a CSP to offer its products cloud based only in the near future. According to the stakeholder, the reason for conducting the PoC was therefore primarily to comply with data protection regulations, especially with a view to Articles 9, 28, 32, 44 et seqq. GDPR and corresponding national law.

To date, the PoC has not been implemented in a productive system. No contract had been negotiated and no personal data has been transported to a cloud. This has to be kept in mind when analysing the following.

#### **1. Pre-contractual phase**

The stakeholder seems aware of GDPR requirements (e.g. DPIA, technical and organisational measures, involving the DPO). The whole concept aims at ensuring the highest level of data protection when using cloud services. According to the stakeholder, only IP addresses would be transported to the cloud but no other data would be made accessible for the CSP.

However, the stakeholder states that data protection is only one argument when choosing a CSP. Functionality and convenience for government tasks are at least as important.

#### **2. Contract with the CSP**

The stakeholder assures that in any case it would secure the government's dispositional sovereignty over the processed data. To this end, before awarding a contract, it would be necessary the CSP accepts the terms set out in a model contract, which had been approved by the competent SA. This would

secure the requirements of Art. 28 GDPR. According to the stakeholder, this is also true with regard to Art. 28(3) (d) GDPR.

The stakeholder informs that there is a model contract negotiated with participation of the federal government and one of the major German digital associations. SCC would be used, according to the respective data being processed.

### 3. International transfers

The stakeholder emphasises, if the concept were implemented, there would be different legal requirements depending on the type of data being processed and the location of the cloud servers. A case-by-case approach would be conducted. The stakeholder would always analyse where the data is being transferred to, what legislations would be applicable insofar and which access options there would be (although, according to the concept, the data transfer should in principle be limited to IP addresses).

## Part III - Actions by the SA

1. Have you taken action (i.e. fact-finding exercises, informal contact, prior consultation, investigation) towards any of the stakeholders concerning the use of cloud-based services prior to launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).
  - No
2. What action(s) are you planning to undertake based on the results of this coordinated action, if any? (E.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)
  - Discussions or awareness raising should take place on the occasion of supervisory measures. Measures will only be taken after leads have been agreed on how to deal with the issue of third-country transfers and thus a reliable framework for supervisory action is established.

## Part IV - Other

1. What is your general impression of the levels of awareness and compliance of the stakeholders you consulted concerning the use of cloud?
  - They are all aware but cannot see a reliable framework to base their actions on? Shutting down CSP applications is de facto not an option.
  - Regarding international data transfer it is stated, that no data transfers to third countries take place because only data centres located in Europe are used. There seems to be little awareness that, at the moment, using US-based cloud services is not usually possible without data transfer to the USA.
  - Standards, contracts and non-GDPR certifications are taken as a basis to choose a cloud provider. A detailed review of the actual processing does not always take place.
2. Are there any other issues or topics that you would like to flag?
3. Are there any leading practices of the stakeholders you have contacted that you would like to share?

## INTRODUCTION

1. This report has been prepared in the context of the EDPB 2022 Coordinated Enforcement Action, which focuses on the use of cloud-based services by the public sector. One of its goals is to explore the challenges that public bodies face in terms of compliance with the GDPR<sup>6</sup>/EUDPR<sup>7</sup>. This includes the procedures for procuring cloud-based services and associated safeguards that must be implemented as well as the contractual and actual compliance with data protection rules, and in particular transfers outside the European Economic Area ('EEA') in view of the Schrems II judgment.<sup>8</sup>
2. The CEF further aims at fostering best practices by supervisory authorities through coordinated guidance and action, thereby ensuring the protection of personal data.
3. This report, along with reports of all other supervisory authorities participating in the Coordinated Enforcement Action, will result in a joint report with aggregated results, generating deeper insight and allowing targeted follow-up at EU level.

## Part I - Statistics

### 1. How many stakeholders have you contacted within the following categories?

- Ministry of the central government
  - Independent public body of the central government
  - Buyer for the central government
  - Publicly-owned company acting as a processor for several central public bodies
  - Ministry of the regional government
  - Independent public body of the regional government
  - Buyer for the regional government
  - Publicly-owned company acting as a processor for several regional public bodies
  - Other, please specify
- 
- **Answer:** In 2022, the EDPS has formally contacted five EU institutions, bodies, offices and agencies ('EU institutions and bodies'), which could be considered equivalent to a "ministry of the central government" or "independent public body of the central government". One of those EU institutions and bodies was a buyer for other EU institutions and bodies, equivalent to a "buyer for the central government". Prior to that, all 69 EU institutions and bodies were contacted in 2020 (more on that in paragraph 35). In addition to that, several more EU institutions and bodies have been contacted informally and have been provided guidance.

---

<sup>6</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) (OJ L 119, 4.5.2016, p. 1).

<sup>7</sup> Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

<sup>8</sup> *Facebook Ireland and Schrems (Schrems II)*, C-311/18, ECLI:EU:C:2020:559.

**2. How many stakeholders have you contacted within the following sectors?**

- Agriculture
  - Defence
  - Digitalisation of the Public Administration/e-Government
  - Economic affairs
  - Education
  - Finance
  - Health
  - Infrastructure
  - Employment
  - Justice
  - Tax
  - Other, please specify
- **Answer:** The EDPS has formally contacted five stakeholders in the digitalisation of the public administration/e-government and justice sectors and one stakeholder in all other listed sectors.

**3. If you have contacted a buyer, for which sectors does this buyer provide its services:**

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government
- Economic affairs
- Education
- Finance
- Health
- Infrastructure
- Employment
- Justice
- Tax
- No specific sector
- Other, please specify

- **Answer:** The buyer provides its services for all of the listed sectors.

**4. If you have contacted a buyer, and if you have this information, please specify the number of stakeholders this buyer provides services for.**

- **Answer:** The buyer provides its services to up to 71 stakeholders.

**5. What was the initial procedural framework of your action?**

- ***Fact finding***
- ***Fact finding + determining follow-up action based on the results***
- ***New investigation<sup>9</sup>***
- ***Ongoing investigations***

- **Answer:** At the launch of the 2022 Coordinated Enforcement Action, we were conducting ongoing investigations.

---

<sup>9</sup> Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.

**6. How many stakeholders indicated that they use CSPs or are planning to do so in the near future (end of 2022)?**

- **Answer:** In the context of the 2020 reporting exercise, 20 stakeholders indicated that they used or planned to use cloud service providers ('CSPs'). We assume that this number has increased since then. In particular, we note that the inter-institutional contracts with the CSPs concluded by the central buyer allow all EU institutions and bodies to use the cloud-based services under those contracts.

**7. Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?**

- Internal organisation (office suites, internal communication, HR, etc.)
- Exercise of public functions (services to citizens, processing citizen's data, etc.)
- **Answer:** All of those stakeholders use CSPs for those two functions, i.e. at least 20 stakeholders (see our response to the preceding question). We note also that the inter-institutional contracts with the CSPs concluded by the central buyer do not make the distinction between those two functions.

**8. For the following commonly identified sectors, please specify if any hyper-scalers<sup>10</sup> are involved (if so please name them) either because they provide the services themselves or because the services are using the infrastructures of these hyper-scalers.**

- Health
- Finance
- Tax
- Education
- Central buyers or providers of IT services
- **Answer:** Yes, Microsoft, Amazon, IBM, OVH for all those sectors.

**9. How many stakeholders took the following actions prior to or during the acquisition of a CSP?**

- Perform a DPIA
- Does the DPIA analyse transfers in details (sometimes called DTIA)
- Contact the DPO for advice
- Perform a general risk analysis
- Contact the SA for advice
- **Answer:** Five EU institutions and bodies have performed a DPIA, contacted the DPO for advice and performed a general risk analysis. Four of those carried out a transfer impact assessment and contacted the EDPS for advice. This is without prejudice to our assessment whether those actions were performed properly.

**10. How many stakeholders (including buyers) take the following actions during the use of the CSP?**

- Monitoring technical and organisational measures to ensure compliance

---

<sup>10</sup> Hyper-scalers provide cloud services at scale. It refers usually to the big cloud providers (Google, AWS, Microsoft ...) on which other services may also depend

- In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g. Schrems II)
- Regular risk assessments
- **Answer:** Five EU institutions and bodies have taken the listed actions. This is without prejudice to our assessment whether those actions were performed properly.

## Part II - Substantive issues

### 1. **Purpose limitation**

- One of the key concerns focused on by the ongoing investigations related to the use of the CSPs is to determine whether the principle of purpose limitation has been properly respected, both contractually and in practice. This includes an examination of compliance with Articles 4(1) (b), 6 and 29(3) EUDPR (equivalent to Articles 5(1)(b), 6(4) and 28(3) GDPR). Moreover, compliance with Article 9 EUDPR, which does not have an equivalent provision in the GDPR, is also scrutinised. That provision permits the transmissions of personal data within the EEA only where this is necessary for a specific purpose in the public interest or for the performance of a task in the public interest.
- In this regard, the investigations seek to establish whether:
  - the purposes for the collection of personal data are explicit and specified and set out in a contract or another legal act;
  - the purposes for further processing are compatible with the purposes for which the data were initially collected;
  - contractual determination of categories of personal data is sufficient so as to allow the purpose for the collection and further processing to be explicit and specified.
- The issue of compliance with the principle of purpose limitation was already the subject of an EDPS investigation in 2019-2020, which concluded with the EDPS making several recommendations (see paragraph 34). The purpose of ongoing investigations is to determine whether those recommendations have been followed as well as to examine compliance related to additional CSPs used by EU institutions and bodies.
- One of the reasons for this and other compliance issues appears to be an imbalance of power between the hyper-scale CSPs and the EU institutions and bodies. In addition, the EU institutions and bodies are in some instances unable to obtain sufficient information in order to carry out proper assessments necessary for the performance of the processing and for the implementation of the required organisational and technical measures (e.g. due to business secrets invoked by certain CSPs).
- As regards differences between the stakeholders, we note that compliance levels are often higher where the EU institutions and bodies have involved the EDPS at an early stage, preferably prior to the initiation of the procurement procedure. This generally applies to all substantive issues.
- EU institutions and bodies concluding agreements with CSPs should ensure that the personal data are sufficiently determined in relation to the purposes for which they are processed and that they are collected for explicit and specified purposes and not further processed for incompatible purposes. This should be done by way of clear and exhaustive provisions stipulated in a contract

concluded pursuant to Article 29(3) EUDPR (Article 28(3) GDPR), as well as organisational and technical measures, as necessary.

## **2. Controller-processor relationship**

- Another key issue is the contractual allocation of the roles of controller and processor, and in particular, whether it corresponds to the factual circumstances. This entails an examination of compliance with Articles 29 and 30 EUDPR (equivalent to Articles 28 and 29 GDPR).
- The ongoing investigations focus on whether the divisions between the roles is appropriately defined in light of the public service character of EU institutions and bodies. As such, the EU institutions and bodies should ensure that the factual circumstances of the processing, including the determination of its purposes and means, are accurately reflected in the allocation of the roles and corresponding responsibilities under the relevant contracts.

## **3. Authorisation AND USE of sub-processors**

- A related issue under examination concerns the engagement and use of sub-processors as regulated by Article 29(1), (2) and (4) EUDPR (equivalent to Article 28(1), (2) and (4) GDPR). This may also result in an infringement of Article 29(3) (d) EUDPR (equivalent to Article 28(3) (d) GDPR). In particular, the investigations seek to establish whether the EU institutions and bodies as controllers have:
  - a meaningful right to withhold authorisation of sub-processors;
  - authorised only the use of sub-processors which provide sufficient guarantees within the meaning of Article 29(1) EUDPR (equivalent to Article 28(1) GDPR);
  - ensured that the contract between the processor and sub-processors sets out the same data protection obligations, as they must be stipulated in the contract between the controller and processor, as required by Article 29(4) EUDPR (equivalent to Article 28(4) GDPR).
- The solutions depend on the specific circumstances of each case, however one potential solution for a controller seeking to gain greater control over the selection of the sub-processors by hyper-scale CSPs might be to define contractually the specific criteria that any new sub-processors must meet, or to define what information the CSPs must provide on proposed new sub-processors. This could allow controllers to anticipate and mitigate risks posed to data subjects better.

## **4. Technical and security measures to mitigate risks**

- Our investigation further seeks to establish whether appropriate security measures of technical and organisational nature have been identified in the controller's security risk assessment and whether they have been made mandatory with respect to all applicable processing operations.
- Such security measures are required, in particular, by Article 33 EUDPR (equivalent to Article 32 GDPR) and by Article 36 EUDPR (no equivalent provision in GDPR). This includes logging, encryption, identification and authentication of users, audits events, incident handling, flaw remediation etc. Particular attention is dedicated to measures that mitigate the highest risks identified.
- In case an infringement is established, the controller should, in particular, ensure that all the necessary security measures are clearly determined as mandatory.

## **5. International transfers**

- Another major area of concern is transfers outside the EEA and the requirements, in particular, of Chapter V EUDPR (similar to Chapter V GDPR) as interpreted by the Schrems II judgment. Our ongoing investigations focus mainly on:
  - the controller's understanding of what transfers are taking place, i.e. the accuracy and completeness of its transfer mapping exercises;
  - transfer impact assessment, i.e. assessing the level of protection in the third country in the context of the specific transfers as to whether supplementary measures are needed and whether any effective supplementary measures exist;
  - implementation of appropriate contractual and other safeguards, including effective supplementary measures where required.
- These issues are interlinked since they have to be properly carried out in sequence. In other words, a complete transfer impact assessment cannot be carried out without first completing proper transfer mapping, nor is it possible to implement effective safeguards without a thorough transfer impact assessment. An important element to take into account is that depending on the nature of the processing, effective supplementary measures may not be available even where they are required to ensure an essentially equivalent level of protection.
- The EUDPR/GDPR, as interpreted by the Court of Justice, do not permit transfers where required supplementary measures are not implemented. In such instances, the EU institutions and bodies should ensure that such transfers do not take place. In some cases, it may be possible to take advantage of a sovereign cloud solution which would not entail transfers outside the EEA nor the application of extra-territorial third-country legislation.
- In order to achieve compliance, the EU institutions and bodies should:
  - carry out an exhaustive transfer mapping exercise in order to identify which personal data are transferred to which recipients in which third countries and for which purposes, including any onward transfers;
  - carry out a complete transfer impact assessment;
  - implement effective safeguards and mitigating measures, including supplementary measures if any are identified in the transfer impact assessment.
- Additionally, EU institutions and bodies can assess alternatives to using a current CSP, which would not result in non-compliant transfers.

## **6. Necessity to use cloud-based services**

- The EDPS has also been paying particular attention to compliance with the data minimisation principle referred to in Article 4(1)(c) EUDPR (equivalent to Article 5(1)(c) GDPR) as well as with data protection by design and by default principles under Article 27 EUDPR (equivalent to Article 25 GDPR) in relation to the use of CSPs. It is incumbent on the controller to choose processing activities that are the least intrusive while still being effective. As regards the selection and use of IT products and services entailing the processing of personal data, the respect for this principle would require making reasonable efforts in seeking alternatives that allow the controller to carry out its tasks effectively while posing lower risk to data subjects.
- In that regard, the controller would have to demonstrate such compliance, as required by the accountability principle referred to in Article 4(2) EUDPR (equivalent to Article 5(2) GDPR) and the controller's obligations specified in Article 26 EUDPR (equivalent to Article 24 GDPR). This implies showing that the selection of the CSP concerned was an outcome of a thorough process assessing

the existence of data protection compliant alternative products and services meeting its specific needs.

### Part III - Actions by the SA

#### 1. **Actions taken prior to the launch of the coordinated action**

- In 2019-2020, the EDPS carried out an investigation into the use of Microsoft's products and services by EU institutions and bodies. Based on that investigation, the EDPS issued its **Findings and Recommendations** to the EU institutions and bodies.<sup>11</sup> This occurred before the Court of Justice handed down the Schrems II judgment, however, many of the identified issues anticipated that ruling. In particular, the recommendations pertained to ensuring that the EU institutions and bodies maintain proper control over the processing activities, particularly in view of the public role of the EU institutions and bodies, as well as control over what data are transferred where and how. Moreover, the EDPS recommended that the EU institutions and bodies put in place appropriate technical measures to stem the flow of personal data sent to the CSPs as well as measures to be taken to ensure compliance with the transparency obligations of EU institutions and bodies towards data subjects.
- In the context of its Schrems II Strategy,<sup>12</sup> the EDPS issued an **order**, in October 2020, to all EU institutions and bodies to complete a transfer mapping exercise identifying which ongoing contracts, procurement procedures and other types of cooperation involve transfers of data, and to report certain results to the EDPS. We also strongly encouraged the EU institutions and bodies to avoid processing activities that involve transfers of personal data to the United States. Following that order, the EDPS has received numerous requests for guidance on proper compliance, which we have provided as informal and formal supervisory opinions.
- In May 2021, the EDPS opened two investigations following the Schrems II judgment.<sup>13</sup> One regarding the use of cloud services provided by Amazon Web Services and Microsoft under Cloud II contracts by EU institutions and bodies, and one regarding the use of Microsoft 365 by the European Commission.
- In July 2021, the EDPS issued an **opinion**<sup>14</sup> in response to a request for prior consultation under Article 40 EUDPR (equivalent to Article 36 GDPR) by an EU institution (the European Central Bank). In that opinion, the EDPS addressed the question whether mitigating measures identified by the institution concerned could be considered sufficient to appropriately address the high risk identified in relation to the envisaged use of Microsoft Dynamics 365. The EDPS concluded that the envisaged measures were insufficient to mitigate those risks. As a consequence, the EDPS found that there were not sufficient guarantees and appropriate safeguards that the processing by the CSP and its sub-processors would meet the statutory requirements and ensure an essentially equivalent level of protection to that guaranteed in the EEA. The EDPS therefore issued a **warning** that the envisaged processing operation was likely to infringe Articles 4(2), 27, 29, 46, and 48 EUDPR (equivalent to Articles 5(2), 25, 28, 44 and 46 GDPR). Moreover, the EDPS made several **recommendations** to assist the institution in ensuring compliant processing.

---

<sup>11</sup> See the [EDPS Public Paper on the Outcome of own-initiative investigation into EU institutions' use of Microsoft products and services](#).

<sup>12</sup> [EDPS Strategy for Union institutions, offices, bodies and agencies to comply with the 'Schrems II' Ruling](#).

<sup>13</sup> [https://edps.europa.eu/press-publications/press-news/press-releases/2021/edps-opens-two-investigations-following-schrems\\_en](https://edps.europa.eu/press-publications/press-news/press-releases/2021/edps-opens-two-investigations-following-schrems_en).

<sup>14</sup> [EDPS Opinion on a prior consultation requested by the European Central Bank on their new customer relationship management system](#).

- In July 2021, the EDPS issued another **opinion**<sup>15</sup> in relation to transfers to a third country. The opinion included guidance on the use of derogations under Article 50 EUDPR (similar to Article 49 GDPR) for transfers carried out in the context of the use of the CSP for the purposes of publishing a newsletter by the EU agency (ENISA). In particular, we highlighted that the agency should assess, in cooperation with the CSP, whether there were alternative newsletter publishing solutions available that do not involve the transfers of personal data to the United States.

## 2. **Actions envisaged or taken after the launch of the coordinated action**

- In April 2022, the EDPS published a **factsheet**<sup>16</sup> in order to share an informal supervisory opinion issued to an EU institution requesting guidance. In that document, the EDPS reminded the EU institutions and bodies of the recommendations issued following its 2019-2020 investigation into the use of Microsoft's products and services by EU institutions and bodies and of its ongoing investigation into the use of Microsoft 365 by the European Commission. The EDPS also recalled the requirements and consequences of the Schrems II judgment as regards the transfers outside the EEA as well as informed them of the 2022 Coordinated Enforcement Action.
- In April 2022, the EDPS also issued a **decision**<sup>17</sup> to an EU agency (Frontex) on its move to a hybrid cloud consisting of Microsoft Office 365, Amazon Web Services (AWS) and Microsoft Azure, following an investigation initiated in June 2020. The investigation looked at compliance with the EUDPR, taking into account EDPS Guidelines on the use of cloud computing services<sup>18</sup> issued in 2018. The EDPS found that the agency had moved to the cloud without a timely and exhaustive assessment of data protection risks and identification and implementation of appropriate mitigating measures. The EDPS also found that the agency had failed to observe the principles of lawfulness and data minimisation. The EDPS therefore issued a **reprimand** for a breach of Articles 4(2), 26 and 27 EUDPR (equivalent to Articles 5(2), 24 and 25 GDPR) as well as an **order** to review and amend the DPIA and the record of processing activities to bring the processing into compliance with the EUDPR.
- In June 2022, the EDPS issued an **opinion** to an EU agency in response to a request for prior consultation on an online platform entailing the use of cloud computing services. The EDPS concluded that the specific risks related to the development and operation of the online platform had not been sufficiently identified. In particular, it recommended that the agency ensure that the contractual framework binds the processor to meet the data protection requirements and that it assess the transfers that the use of cloud services may entail.
- In October 2022, the EDPS issued a decision pursuant to Article 58(3) (e) EUDPR (equivalent to Article 58(3) (h) GDPR) conditionally authorising the use of contractual clauses for transfers of personal data between an EU institution (the Court of Justice of the EU) and a CSP (Cisco). The EDPS authorised their use until 31 October 2024 given, inter alia, the essential function that the institution carries out in the EU, the commitment by the institution and the CSP to comply with the EUDPR and the need for a certain period of time to implement the necessary measures. However, the EDPS set a number of strict conditions to be met in order to remedy the remaining shortcomings and to ensure an essentially equivalent level of protection. This decision follows a

---

<sup>15</sup> [EDPS Opinion on transfers to a third country resulting from the use of a newsletter service by ENISA](#).

<sup>16</sup> [https://edps.europa.eu/system/files/2022-04/22-04-29\\_ongoing-investigation-into-the-use-of-m365-by-euis\\_en.pdf](https://edps.europa.eu/system/files/2022-04/22-04-29_ongoing-investigation-into-the-use-of-m365-by-euis_en.pdf).

<sup>17</sup> [EDPS Decision concerning the investigation into Frontex's move to the Cloud](#).

<sup>18</sup> [EDPS Guidelines on the use of cloud computing services by the European institutions and bodies](#).

previous EDPS decision of August 2021<sup>19</sup> authorising the use of the contractual clauses in question for 13 months.

- Furthermore, in addition to pending requests for prior consultation, the EDPS intends to issue decisions once the ongoing investigations have been concluded, and use its corrective powers where necessary. It is envisaged to issue those decisions in 2022/2023.

## Part IV - Other

### 1. **General impression**

- The levels of awareness and compliance appear to be relatively low. However, we have reasons to presume that following the EDPS' order of 2020 to carry out a transfer mapping exercise to all EU institutions and bodies, as well as further guidance provided, the overall awareness and compliance in that regard have risen. Nonetheless, the need for improvement remains, in particular as regards the proper implementation of measures that will, in addition to contractual measures, mitigate the risks arising from third-country legislation.

### 2. **Leading practices**

- The EDPS (as a supervisory authority) and other EU institutions and bodies (as controllers) have been closely involved in certain inter-institutional procurement procedures<sup>20</sup> relating to the cloud services. This has allowed the relevant data protection and security requirements to be integrated already in the procurement notice and selection and were therefore reflected in the subsequent contracts. Since many data protection issues stem already from the procurement stage, such practice effectively contributes to the proper implementation of the relevant rules. The EU institutions and bodies that were already closely involved in such procedures before Schrems II judgment, have become even more involved following that judgment. In particular, this concerns greater involvement in clarifying the situations in which cloud services may be used and what safeguards and measures are already available, as well as in the development of new measures additional to those already in place.
- In addition, the EDPS as a controller initiated an informal consultation concerning the procurement of Software-as-a-Service and hosting services from an EU-based provider. The EDPS as a supervisory authority made recommendations to the controller on data protection requirements within the procurement procedure, on the selection of providers by using relevant data protection criteria and guarantees to be required from the provider, including ensuring that processing only takes place in the EEA and that extra-territorial third-country legislation does not apply. Furthermore, we advised the controller on technical, organisational and security measures to be implemented, additional contractual clauses to be included into the model inter-institutional contract to be led by the EDPS, and on the involvement of other EU institutions and bodies. Following the procurement procedure, the SaaS will be based on Nextcloud's software and will be provided and hosted by TAS France.
- The EDPS also welcomes the requests of EU institutions and bodies for guidance, as well as requests for prior consultation or authorisation where required in accordance with the relevant statutory provisions. Such requests of EU institutions and bodies are an indication of an elevated level of awareness of the impact that the processing in the cloud and international transfers have on individuals. This is a crucial step towards compliance with the applicable EU data protection law.

---

<sup>19</sup> [EDPS Decision authorising temporarily the use of ad hoc contractual clauses between the Court of Justice of the EU and Cisco for transfers of personal data in the Court's use of Cisco Webex and related services.](#)

<sup>20</sup> Both before and after the Schrems II judgment.

## Part I – Statistics

**1. How many stakeholders have you contacted within the following categories?**

- Ministry of the central government: **1**
- Independent public body of the central government: **2**
- Buyer for the central government: **n/a**
- Publicly-owned company acting as a processor for several central public bodies: **n/a**
- Ministry of the regional government: **n/a**
- Independent public body of the regional government: **1**
- Buyer for the regional government: **n/a**
- Publicly-owned company acting as a processor for several regional public bodies: **n/a**
- Other, please specify: **n/a**

**2. How many stakeholders have you contacted within the following sectors?**

- Agriculture: **n/a**
- Defence: **n/a**
- Digitalisation of the Public Administration/e-Government: **n/a**
- Economic affairs: **n/a**
- Education: **1**
- Finance: **n/a**
- Health: **1**
- Infrastructure: **1**
- Employment: **n/a**
- Justice: **n/a**
- Tax: **n/a**
- Other, please specify: **1 municipality**

**3. If you have contacted a buyer, for which sectors does this buyer provides its services:**

- n/a

**4. If you have contacted a buyer, and if you have this information, please specify the number of stakeholders this buyer provides services for:**

- n/a

**5. What was the initial procedural framework of your action?**

- Fact finding
- Fact finding + determining follow-up action based on the results
- New investigation<sup>21</sup>
- Ongoing investigation

**6. How many stakeholders indicated that they use CSPs or are planning to do so in the near future (end of 2022)?**

- All 4 stakeholders indicated that they use CSPs.

---

<sup>21</sup> making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred

7. Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?
- Internal organisation (office suites, internal communication, HR, etc.) : 3
  - Exercise of public functions (services to citizens, processing citizen's data, etc.): 4 (all responding stakeholders).
  -
8. For the following commonly identified sectors, please specify if any hyperscalers<sup>22</sup> are involved (if so please name them) either because they provide the services themselves or because the services are using the infrastructures of these hyper-scalers
- Health: Microsoft, Fujitsu
  - Finance: n/a
  - Tax: n/a
  - Transport: Microsoft, Amazon
  - Education: Microsoft, Google, Adobe, Zoom, Facebook, Instagram
  - Central buyers or providers of IT services: n/a
9. How many stakeholders took the following actions prior to- or during the acquisition of a CSP?
- Perform a DPIA: 1
  - Does the DPIA analyse transfers in details (sometimes called DTIA): Content of the DPIA is unknown, as it was not asked to submit.
  - Contact the DPO for advice: 3
  - Perform a general risk analysis: based on stakeholder's answers, we are not aware (or can't be sure) that written risk analysis (from the point of data processing) are performed.
  - Contact the SA for advice: 0
10. How many stakeholders (including buyers) take the following actions during the use of the CSP?
- Monitoring technical and organisational measures to ensure compliance: 4
  - In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g. Schrems II): 0. As a rule of thumb, stakeholders rely on CSP standard agreement and SLA terms. No supplementary measures are adopted and regulatory landscape is not monitored. Only one stakeholder mentioned that CSP has implemented SCC (EC 2021/914). Stakeholders experience lack of awareness if and which personal data might be transferred to third country.
  - Regular risk assessments: based on answers we cannot be sure that regular risk assessment is performed.

## Part II – Substantive issues

- The Supervision Authority participated in the joint surveillance of the EDPB in the form of fact finding monitoring. The aim was, in particular, to map the practice of using public cloud services in selected institutions and to what extent the authorities have understood the impact of the use of cloud services on data protection and people's privacy. We have had no further contact with the data controllers following the answers to the questions. We may start with follow-up activities

---

<sup>22</sup> Hyper-scalers provide cloud services at scale. It refers usually to the big cloud providers (Google, AWS, Microsoft ...) on which other services may also depend

in the beginning of next year. As a result, no solutions and corrective actions could be implemented yet in relation to the issues raised by the monitoring.

- The responses to the monitoring exercise identified the following potential problems and bottlenecks:
1. **Data processors lack clarity on whether and what personal data are processed in cloud services and to what extent**
    - Understanding the processing of personal data and its scope is one of the most important components of legitimate applicability of the GDPR. If personal data is not processed in the information systems, the GDPR does not apply. If personal data exists, the scope of applicability of the GDPR depends, for example, on the sensitivity of the data, the volume of the data or whether the systems processing the data are located in third countries. The context is therefore of paramount importance.
    - Three out of four respondents made it clear that personal data is processed in cloud services. Of these, only two authorities indicated that the data of both employees and other persons (publicity) are processed in cloud services. One authority's reply gave the impression that only data from cloud administrators is processed. The information was also contradictory at times because, for example, for the question of whether DPIA was also carried out, there were responses that since the volume of personal data processed is currently small, DPIA was not deemed necessary.
    - According to one of the respondents, there are also special categories of personal data among the data processed.
    - According to one of the respondents, data processed in cloud services only concerns employees. However, it is difficult to accept this argument as the service used included, for example, MS 365, Google, Zoom and Facebook. If an institution uses e.g. cloud-based office software, the documents that are to be processed or compiled certainly do not contain only staff-related data. The authorities also communicate very much with public in the context of their public tasks. On a daily basis, individuals also turn to authorities with various problems and questions. Often these are sensitive issues of individuals, including minors.
  2. **No data protection impact assessment has been carried out prior to the use of cloud services**
    - This is a major problem for all respondents. Common reasons why no impact assessment was made were that there was no personal data; that the service provider had already done so and trusted it; or that it was not a high-risk data processing. Only one of the respondents said they had done it. However, since there was no obligation to transmit impact assessment documents in the context of the monitoring, it is difficult for us to say whether the impact assessment had been carried out in accordance with the requirements of Article 35 GDPR.
    - It is important to note that if an impact assessment has been carried out by any cloud service provider, this is usually an analysis of the overall risks. Often only from the viewpoint of information security and information system as a whole. However, the potential risks of data protection for the people involved in the service have not been assessed. After all, the service provider is not aware of the organizational or national legal obligations of the body using the service.

- It was also clear from the answers that when entering the service, the first priority of the institution was to find solutions primarily for organizational needs. Often the only goal is to save the costs to infrastructure and optimization.

### **3. The use of the service is based on the service provider's standard contract and the service level agreement (SLA)**

- According to only one respondent, there was the impression that the institution had pre-contractual negotiations with the service provider. An adapted SLA is also concluded if the SLA by the service provider does not meet the expectations. Allegedly, the institution has the right to control and audit the cloud service provider under the contract.
- The remaining three respondents rely on the service provider's standard terms of the contract. Thus, the authorities have generally failed to comply with the requirement of Article 28 of the GDPR. However, in the case of unilateral acceptance of the contract terms of the service provider, it is difficult for the authorities to ensure compliance with other provisions of the GDPR, for example with Articles 5, 12, 13, 14, 21, 24, and 32 of the GDPR. The service provider may contractually assume the rights to process datasets relating to the activities of the institution for its own purposes. Often, these goals are deliberately formulated in such a general way that the understanding of what a cloud enterprise actually does and how much a cloud enterprise does is incomprehensible. Authorities take very lightly the service provider's claims that the contract complies with GDPR requirements.

### **4. Lack of awareness of sub-delegated processors**

- As a general rule, all cloud services use external partners, i.e. sub-processors, who process data on the basis of the processor's authorization pursuant to Article 29 of the GDPR. Be it to ensure a component or a function of the service. This is particularly relevant in ensuring information security, where different firewall solutions or distribution of network loads are carried out by external parties. Therefore, it is of paramount importance for the authority using cloud service, as responsible for compliance with GDPR requirements, to understand and know which parties are involved in data processing.
- Monitoring confirmed our practice so far that the knowledge of data processors in sub-delegated processing is lacking or none. Three out of four respondents said they did not know which sub-processors are being used by the cloud service provider. One respondent claimed that sub-processors were not used (although they were the two largest cloud services in the world). Only one respondent provided a list of sub-processors in the cloud service provider's contract.
- In the case of sub-processors, the lack of knowledge of the region in which the data processing is carried out is also a major problem. This can occur in third countries. Despite the lack of knowledge of sub-processors by controllers, the sub-processor under Article 29 GDPR is obliged to process the data under the instructions of the controller.

### **5. Lack of awareness of telemetry/diagnostic data processing**

- Only one out of four respondents indicated that cloud services do not process telemetry or diagnostic information. The other three replied that such processing takes place, but the data processed does not include personal data. The reason was to ensure the quality of the service or to identify errors. Two respondents were aware that, in the context of the processing of cloud telemetry data, data transfers to third countries take place on the basis of Chapter V of the GDPR.

**6. Insufficient due diligence in implementing additional safeguards for transfers to a third countries**

- According to the three respondents, there is no transfer to third countries, as they rely on the cloud service provider's confirmation and the possibility to select a data centers in the European Union for data processing. Only one respondent says that data transfer to third countries is taking place. According to the same respondent, the cloud service provider uses standard contractual clauses under Commission Implementing Decision 2021/914. It is not specified whether the contract is the controller-processor or the processor-processor.

**Part III – Actions by the SA**

1. Have you taken action (i.e. fact-finding exercises, informal contact, prior consultation, investigation) towards any of the stakeholders concerning the use of cloud-based services prior to launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).
  - No, we haven't taken any action towards any of the stakeholders concerning the use of cloud based services prior to launching the coordinated action.
2. What action(s) are you planning to undertake based on the results of this coordinated action, if any? (E.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)
  - Specific actions are not planned yet. It would be under discussion which are our focus topics for 2023 work plan.

**Part IV – Other**

1. What is your general impression of the levels of awareness and compliance of the stakeholders you consulted concerning the use of cloud?
  - Based on sweep answers we have received, level of awareness and compliance of the stakeholders is not sufficient.
2. Are there any other issues or topics that you would like to flag?
  - In Estonia, the legal framework for the use of public cloud services in the public sector are being prepared by the Ministry of Economic Affairs and Communications.
3. Are there any leading practices of the stakeholders you have contacted that you would like to share?
  - No

## Part I – Statistics

### 1. How many stakeholders have you contacted within the following categories?

- Ministry of the central government : 3
- Independent public body of the central government : 4
- Buyer for the central government : 1 (**the buyer is a ministry of the central government – Ministry of Digital Governance and is included in the number above for the ministries contacted**)
- Publicly-owned company acting as a processor for several central public bodies
- Ministry of the regional government
- Independent public body of the regional government
- Buyer for the regional government
- Publicly-owned company acting as a processor for several regional public bodies
- Other, please specify

### 2. How many stakeholders have you contacted within the following sectors?

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government : 1
- Economic affairs
- Education
- Finance
- Health : 2
- Infrastructure
- Employment : 3
- Justice
- Tax
- Other, please specify : Immigration and Asylum : 1

### 3. If you have contacted a buyer, for which sectors does this buyer provides its services:

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government
- Economic affairs
- Education
- Finance
- Health
- Infrastructure
- Employment
- Justice
- Tax
- No specific sector: **The Ministry of Digital Government offers cloud services through the governmental Cloud (G-Cloud) to public bodies of every sector.**
- Other, please specify

**4. If you have contacted a buyer, and if you have this information, please specify the number of stakeholders this buyer provides services for:**

- Approximately 150 public bodies are hosted in G-Cloud (information taken from the buyer's website: <https://www.gsis.gr/ggpsdd/orama-apostoli>)

**5. What was the initial procedural framework of your action?**

- Fact finding
- Fact finding + determining follow-up action based on the results: **The initial framework was fact finding and determining follow-up action based on the results**
- New investigation<sup>23</sup>
- Ongoing investigation

**6. How many stakeholders indicated that they use CSPs or are planning to do so in the near future (end of 2022)?**

- All 7 of them (the 5 stakeholders contacted and 2 more, for which the Ministry of Labour and Social Affairs also sent answers to the questionnaire)

**7. Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?**

- Internal organisation (office suites, internal communication, HR, etc.) : **6**
- Exercise of public functions (services to citizens, processing citizen's data, etc.) : **7**

**8. For the following commonly identified sectors, please specify if any hyperscalers<sup>24</sup> are involved (if so please name them) either because they provide the services themselves or because the services are using the infrastructures of these hyper-scalers**

- Health: **Yes (Microsoft)**
- Finance: **Yes (Oracle, Microsoft 365)**
- Tax: **Yes (Oracle, Microsoft Azure, Microsoft 365)**
- Education
- Central buyers or providers of IT services: **Yes (Microsoft, Oracle)**
- Other: **Employment (Amazon)**

**9. How many stakeholders took the following actions prior to- or during the acquisition of a CSP?**

- Perform a DPIA : **1**
- Does the DPIA analyse transfers in details (sometimes called DTIA) : **Yes**
- Contact the DPO for advice : **3**
- Perform a general risk analysis: **None**
- Contact the SA for advice: **None**

**10. How many stakeholders (including buyers) take the following actions during the use of the CSP?**

- Monitoring technical and organisational measures to ensure compliance: **2**
- In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g. Schrems II). : **None**

---

<sup>23</sup> making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred

<sup>24</sup> Hyper-scalers provide cloud services at scale. It refers usually to the big cloud providers (Google, AWS, Microsoft ...) on which other services may also depend

- Regular risk assessments : 2

## Part II – Substantive issues

### 1. Lack of a general risk assessment and/or DPIA

#### 1.1. Short description:

- According to the questionnaire replies, the CSPs are selected as processors or sub-processors without a general risk assessment.
- With one exception, the questionnaire respondents have not carried out a DPIA or have not asked for a DPIA from the CSP prior to acquiring cloud-based services. Regarding the exception, one public body performed DPIAs for two (2) separate systems after the CSP selection. In this case, the first DPIA has not examined the risks arising from the use of cloud services, while the second suggests specific measures to minimize the risks associated with the use of cloud services, but it is not clear if the controller has taken such measures.
- For the selection of the Government Cloud (G-Cloud) (without a DPIA), a common reason put forward by public bodies is the mandatory use of G-Cloud according to Law 4727/2020 Art. 87 par.4 (as amended)<sup>25</sup>. Another reason put forward by one public body is the processing of a very limited amount of special categories of personal data. Other reasons include the Tier-3 architecture of G-Cloud and its preparation for the acquisition of the ISO 27001 certification.
- In the case of the hyper-scalers, the reasons for their selection include the following: ease of use, expertise and high technological solutions provided, the certifications that hyper-scalers possess (for Microsoft ISO 27001, 9001, 27017, 27018, 27701, 22301 and for Oracle ISO 27001, 27017, 27018, and 27701).

#### 1.2. Which provisions of the GDPR this concerns:

- Articles 24, 28 and 35 GDPR

#### 1.3. Why this has been an issue for the stakeholders :

- The lack of a general risk assessment and/or a DPIA, where necessary, results to the inability of stakeholders to identify and effectively address the risks related to the processing of personal data in the use of cloud services. This deficiency, together with the lack of awareness suggests that stakeholders may face difficulties fulfilling their accountability obligation to use only processors providing sufficient guarantees, according to Art. 28 (1) GDPR.

#### 1.4. Differences between stakeholders:

- Most of the public bodies our SA contacted have not performed any kind of risk assessment before or after acquiring a CSP. Only one public body has carried out DPIAs in two cases with the specific issues as described above.

#### 1.5. Potential solutions to this issue by the SA or the stakeholders:

---

<sup>25</sup> “All central electronic applications and central information systems maintained by all Ministries [...] public entities [...] independent authorities [...etc.] which concern transactions with natural or legal persons or legal entities and the public administration, must be installed in the Public Sector Government Cloud by 1st January 2023. The Government Cloud (G-Cloud) infrastructures of the above entities are transferred and become the property of the General Secretariat of Information Systems for Public Administration for this purpose”.

- A possible solution for the stakeholders would be to carry out a DPIA, at least “ex post” on the use of cloud services, in order to determine any necessary supplementary technical and organizational measures. Another possible solution would be for the central buyer to perform a basic DPIA as a whole, taking into account Law 4727/2020 Art. 87 par.4 (as amended).

## **2. Not fully clear role of the parties, including resellers and intermediaries**

### **2.1. Short description:**

- There is not a common understanding among the stakeholders about the roles of the parties involved in the use of cloud services.
- According to most questionnaire responses, the public bodies act as controllers and the CSPs (central buyer, hyper-scalers) as processors or sub-processors. In some cases, public bodies consider the central buyer to be an independent data controller or a joint controller, because it has the ability to decide on the means of the processing and the selection of sub-processors for providing the G-Cloud services<sup>26</sup>.
- The central buyer itself reported that it acts as processor for providing the G-Cloud services to public bodies, with hyper-scalers (Microsoft, Oracle) as sub-processors for cloud services.
- The role of the hyper-scalers is also not clear regarding the processing of telemetry/diagnostic data that takes place for their own purposes. One public body considered to be a joint controller with Microsoft for the use of Office 365 Suite, because the CSP decides independently on the means of the processing but when our SA asked for further clarifications, this body changed its opinion and answered that Microsoft is a processor.
- The contracts submitted to our SA revealed various relationships. One public body submitted a Microsoft Business and Service Agreement signed between the public body and Microsoft Ireland Operations Limited incorporating the Microsoft Products and Services Data Protection Addendum (DPA) by reference. In another case, the hyper-scalar Amazon Germany is the sub-processor of a consulting company acting as processor for the public body, but without in fact offering cloud services itself (indirect involvement with the hyper-scalar).
- In the other cases with hyper-scalar involvement (Oracle, Microsoft), a contract exists between the controller (direct involvement) or processor (indirect involvement) and the reseller of the hyper-scalar. The reseller is selected through a public procurement procedure and the contract is established after the selection. The role of the reseller (according to the provisions of the GDPR) is not clear and not defined in the contract. It is evident from the questionnaire responses that the role of the resellers/intermediaries is not known to all public bodies.

### **2.2. Which provisions of the GDPR this concerns:**

- Articles 4 (7), (8), 26, 28.1 GDPR

---

<sup>26</sup> According to article 85 of law 4727/2020, among the responsibilities of the central buyer is to acquire cloud services, in total for all public bodies, by priority relative to other technological solutions, for several purposes including the provision of cloud services to public bodies. Also, according to article 28 par. 3 of law 4623/2019, the central buyer is responsible, among others, for the design, development, extension and productive operation of central Governmental Cloud infrastructures, in total for all Public Administration, with the goal of hosting all applications in the central G-Cloud infrastructures of public administration.

### **2.3. Why this has been an issue for the stakeholders:**

- Without clear roles of the parties involved, the public bodies are unable to identify and fulfill their responsibilities arising from the GDPR. The contracts between the parties might miss important elements regarding the processing of personal data or even include incorrect ones. The selection of the CSP becomes difficult, as it is not clear, which party has the responsibility to perform a general risk assessment and decide the selection criteria. In case data subjects exercise their rights regarding data processing in the cloud, the public bodies might not be able to respond to them appropriately. They might also not be able to fulfill their accountability obligation or respond accordingly to the SA.

### **2.4. Differences between stakeholders:**

- The differences between stakeholders are presented in the short description above.

### **2.5. Potential solutions to this issue by the SA or the stakeholders:**

- The roles of the involved parties should be clearly and unequivocally determined and precisely defined in the contract. To this end, public bodies should clearly establish their role relative to the use of cloud services, possibly through an internal assessment. In addition, adequate information from the CSP and DPO consultancy are important elements so that stakeholders become aware of their responsibility and be able to distinguish and evaluate properly their roles in the processing in order to select a CSP according to the provisions of the GDPR.

## **3. Difficulty in negotiating or changing terms of the contract with the CSP**

### **3.1. Short description:**

- The questionnaire replies revealed difficulty of public bodies in negotiating terms or changing the terms of the contract with the CSPs. The terms of the contract are usually predetermined by the CSP.
- The answers provided to the questionnaire regarding the contract with the CSP merely quote parts of Microsoft's DPA, thus indicating either lack of knowledge by stakeholders and/or difficulty in negotiating terms.
- Regarding the possibility of termination or reversibility of the contract, most stakeholders refer to Microsoft's standard terms or answer negatively (either it has not been checked by the public body or such a possibility is not provided). Only one stakeholder answered positively without further explanation.
- The DPA contains information on the processing that Microsoft undertakes as a processor. The DPA is incorporated into the (volume or enterprise) licensing agreement and applies to each customer, irrespectively of products or services. This standard DPA may not suffice as the contract envisaged in article 28 GDPR. More precisely, the DPA Statement that "*the Customer's licensing agreement, including the DPA Terms, along with the product documentation and Customer's use and configuration of features in the Products, are Customer's (as a Controller) complete documented instructions to Microsoft (as a Processor) for the processing of Personal Data*", is too generic and vague to constitute the documented instructions of Article 28(3) GDPR. Moreover, the categories of personal data ("*data generated, derived or collected by Microsoft, including data sent to Microsoft as a result of a Customer's use of service-based capabilities or obtained by*

*Microsoft from locally installed software*<sup>27</sup>) and the purposes for which Microsoft acts as an independent data controller are very broad and not sufficiently explained.

The same applies regarding Oracle as processor. The Data Processing Agreement for Oracle Services incorporates the European DPA Addendum which makes reference to the Oracle Processor Code (Binding Corporate Rules for Processors) regarding cross-border data transfers<sup>28</sup>. The Oracle Privacy Code applies to “*Personal Information of Customer Individuals subject to EEA Data Protection Laws and Processed by Oracle on behalf of its Customers in its role as a Processor in the course of delivering Services*”.<sup>29</sup> The above are standard common documents and apply to all controllers independently of the specific processing. For example, it is not clear and sufficiently explained why and when it is necessary for Oracle to collect data about customer end users, employees, job applicants, end-customers and clients for its own purposes.

### **3.2. Which provisions of the GDPR this concerns:**

- 26, 28 (1), 28 (3), 29

### **3.3. Why this has been an issue for the stakeholders:**

- In many cases, CSPs keep a level of control over the processing that may exceed the role of the processor. If the public bodies have no chance to negotiate such terms, it may be difficult for them to keep determining the purposes and the means over the processing of personal data, and therefore they may not be able to fulfill their obligations as controllers, according to the accountability principle.

### **3.4. Differences between stakeholders:**

- The differences are as described above. Generally, there have been no significant differences found, about the fact that most answers were copied directly from the CSPs standard texts.

### **3.5. Potential solutions to this issue by the SA or the stakeholders:**

- A possible solution would be to investigate whether there is a possibility for public bodies to engage into negotiations with the CSPs, in order to change or insert specific provisions in the contract, with the aim of retaining control over personal data processing and in case this is not feasible, to consider choosing another CSP.

## **4. Lack of a contract or other legal act according to Art. 28/26 GDPR**

### **4.1. Short description:**

- According to the questionnaire replies provided by the participating public bodies, a contract or other legal act, pursuant to article 28(3) GDPR, has not been established between each of them and the central buyer.
- In two cases, the contract with the reseller contains an Appendix for the protection of personal data, pursuant to Art. 28 (3) GDPR. However, in two other cases, the contract with the reseller

---

<sup>27</sup> <https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA>

<sup>28</sup> According to Oracle: ‘Oracle’s BCR-p (also called the ‘Oracle Processor Code’) has been integrated into a new European DPA Addendum, which was added to the new DPA. The European DPA Addendum bundles all GDPR-specific information requirements for data processing agreements, while the DPA describes the general processing terms for all customer personal information globally’. (Source: <https://www.oracle.com/be/a/ocom/docs/corporate/dpa-bcr-statement-of-changes-062619.pdf>)

<sup>29</sup> <https://www.oracle.com/a/ocom/docs/corporate/bcr-privacy-code-051719.pdf>

refers explicitly to specific future agreements/contracts, to fulfill the requirements of Art. 28(3) GDPR, but such contracts were not presented to our SA.

- In all cases with a reseller contract, none of the stakeholders has submitted to our SA an SLA or a licensing agreement with the hyper-scaler. So, this part of the relationship is missing.

#### **4.2. Which provisions of the GDPR this concerns:**

- Articles 24, 26, 28 (3) GDPR

#### **4.3. Why this has been an issue for the stakeholders:**

- Without a proper contract or other legal act in place, the processing on behalf of the controller is not adequately determined. This deficiency makes it difficult for the public bodies to comply with their obligation arising from Art. 28 (1) GDPR, to “use only processors providing sufficient guarantees” that the processing meets the requirements of the GDPR.

#### **4.4. Differences between stakeholders:**

- The differences between stakeholders are presented in the short description above. Overall, no differences were identified among respondents in that they all referred to the standard, predetermined terms of the CSPs. In addition, no differences were found among the participating public bodies concerning the lack of a contract/other legal act with the central buyer as processor containing the terms described in Art. 28.3 GDPR.

#### **4.5. Potential solutions to this issue by the SA or the stakeholders:**

- In the cases where the contract refers to a future specific agreement between the parties, regarding the processing of personal data, such a specific agreement should be negotiated and signed, as soon as possible. Concerning the hyper-scalers and/or their resellers, the relevant contract should be made complete in accordance with the provisions of the GDPR and specific to the processing of each case (not common in all cases independently of the characteristics of the processing).

### **5. Difficulty regarding the freedom of choice of sub-processors**

#### **5.1. Short description:**

- Most public bodies seem to have no control over and cannot object meaningfully to the use of sub-processors or to changes of sub-processors at all or at least without risking a potentially critical loss of service.
- More specifically, the questionnaire respondents either provided no answer at all regarding sub-processors, or referred to the online list with the sub-processors of Microsoft<sup>30</sup>. This indicates that their knowledge is limited to the publicly available information by Microsoft and that they do not have control over the use of sub-processors, such as knowing exactly which one is involved in their particular usage of the cloud or having the chance to object to a specific sub-processor. Besides, the "Microsoft Cloud Services Sub-processors List" does not offer to the Controller a sufficient and clear overview of the sub-processors involved in its processing activities, since:

---

<sup>30</sup>

[https://servicetrust.microsoft.com/ViewPage/TrustDocumentsV3?command=Download&downloadType=Document&downloadId=ede6342e-d641-4a9b-9162-7d66025003b0&tab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913\\_Subprocessor\\_List](https://servicetrust.microsoft.com/ViewPage/TrustDocumentsV3?command=Download&downloadType=Document&downloadId=ede6342e-d641-4a9b-9162-7d66025003b0&tab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913&docTab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913_Subprocessor_List)

- The above list does not contain adequate information on the location of data as it includes only the corporate location and not the exact location where the processing takes place.
- This list does not contain information of the chain of sub-processors.
- This list contains only reference to “customer data” and/or “pseudonymous data” without specifying the specific categories of personal data processed.
- In the case of the central buyer, public bodies don’t have any control over the selection and use of sub-processors, because the central buyer chooses sub-processors through central governmental agreements (article 85 of law 4727/2020, article 28 par. 3 of law 4623/2019), while public bodies are legally bound to use the G-Cloud.

#### **5.2. Which provisions of the GDPR this concerns:**

- Articles 28(1), 28(2) GDPR

#### **5.3. Why this has been an issue for the stakeholders:**

- This deficiency makes it difficult for public bodies to comply with their obligation arising from Art. 28(1) GDPR, to *“use only processors providing sufficient guarantees”* so that the processing meets the requirements of the GDPR. The fact that public bodies have actually no control over the engagement of processor and sub-processors makes it difficult for them to ensure that the processing is compliant with the provisions of the GDPR, especially regarding transfers to third countries. Moreover, it is possible that, when a general authorization is provided, according to Art. 28(2) GDPR, the public body has no meaningful right to object, since the contract does not describe an efficient objection procedure (timeline, consequences etc.).

#### **5.4. Differences between stakeholders:**

- This issue seems to be common among public bodies as in all cases a hyper-scaler is involved (either directly as processor or indirectly as sub-processor of the central buyer). The public bodies do not have sufficient knowledge or control over the sub-processors involved in the processing or the extent of the processing except from general information made available by the hyper-scaler. A difference has been identified between the CSPs Microsoft and Oracle: While Microsoft does not provide enough information regarding the right to object to new sub-processors (the contract merely repeats the text of Art. 28 (2) GDPR), Oracle (Art. 4.3 of the “European DPA Addendum”) describes a timeline (notification period) and foresees that in case of an objection *“Oracle and Customer will work together in good faith to find a solution to address such objection, including making the Services available without the involvement of such Third Party Sub-processor”*.

#### **5.5. Potential solutions to this issue by the SA or the stakeholders:**

- The stakeholders should check with their CSPs to what extent and depth they can be informed about the specific sub-processors engaged in their processing activities, and under which provisions they can exercise their right to object according to Art. 28(2) GDPR.

### **6. Difficulty in determining technical and organisational measures to frame international transfers and access by foreign public authorities**

#### **6.1. Short description:**

- Regarding international transfers, the questionnaire respondents provided answers by referring to the relative standard online texts of the hyper-scalers without specifying the details of transfers pertaining to their own data/systems.
- All questionnaire respondents declared that they have not received any access requests by USA Authorities.

- Regarding Microsoft, although Datacenters within the EU are used, respondents mentioned that, transfers of personal data, including telemetry/diagnostic data, to the US and third countries are based on the terms of the DPA and the information provided online for Office 365<sup>31</sup> and Azure<sup>32</sup> services. Microsoft collects pseudonymized data of the users managing the Azure infrastructure.
- Regarding Oracle, respondents mentioned that personal data (mostly financial data for tax purposes) are stored in the infrastructures of the central buyer within the country. The storage takes place in an automated manner on physical media (disks etc.) within the datacenters of the central buyer and the data is not transmitted outside of these datacenters by Oracle, either manually or automatically. Only systemic telemetry/diagnostic data is collected by the Oracle CSP, by default, through automated processes from the servers of the CSP. The telemetry/diagnostic data collected by Oracle is pseudonymized and limited to administrators' data.
- Detailed information on how the pseudonymization takes place from the CPS (Microsoft, Oracle) is not available and it is not clear whether appropriate safeguards are met.
- According to the section 'Data Transfers and Location' of the Microsoft DPA, "Taking into account such safeguards, Customer appoints Microsoft to transfer Customer Data, Professional Services Data, and Personal Data to the United States or any other country in which Microsoft or its Sub-processors operate and to store and process Customer Data, and Personal Data to provide the Products, except as described elsewhere in the DPA Terms". All transfers are governed by the 2021 Standard Contractual Clauses of the European Commission implemented by Microsoft. It is a processor to processors SCC signed between Microsoft Ireland Operations Limited and Microsoft Corporation.
- None of the questionnaire respondents has examined or negotiated supplementary technical and organizational measures. They only provide information to the measures that the CSP is capable to implement according to the available standard texts without specifying whether they have assessed the application of such measures. One questionnaire respondent mentioned that the negotiation of such supplementary measures is a long process, which would require to analyze, design and implement specific measures in its own environment and to amend the relevant legal texts.

#### **6.2. Which provisions of the GDPR this concerns:**

- Articles 44-47 GDPR

#### **6.3. Why this has been an issue for the stakeholders:**

- Unless the public bodies assess substantially whether specific technical and/or organizational measures should be applied, appropriate for their specific needs, they cannot efficiently limit personal data transfers in a way that is compliant with the provisions of Articles 44-47 GDPR: According to the Appendix C of the Microsoft DPA, "*In the event Microsoft receives an order from any third party for compelled disclosure of any personal data processed under this DPA, Microsoft shall: a. use every reasonable effort to redirect the third party to request data directly from*

---

<sup>31</sup> Office 365 - <https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-dpia-office365>

<sup>32</sup> <https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-dpia-azure>,  
[https://azure.microsoft.com/mediahandler/files/resourcefiles/achieving-compliant-data-residency-and-security-with-azure/Enabling\\_Data\\_Residency\\_and\\_Data\\_Protection\\_in\\_Azure\\_Regions-2021.pdf](https://azure.microsoft.com/mediahandler/files/resourcefiles/achieving-compliant-data-residency-and-security-with-azure/Enabling_Data_Residency_and_Data_Protection_in_Azure_Regions-2021.pdf)

*Customer; b. promptly notify Customer, unless prohibited under the law applicable to the requesting third party, and, if prohibited from notifying Customer, use all lawful efforts to obtain the right to waive the prohibition in order to communicate as much information to Customer as soon as possible; and c. use all lawful efforts to challenge the order for disclosure on the basis of any legal deficiencies under the laws of the requesting party or any relevant conflicts with applicable law of the European Union or applicable Member State law.”* But, according to Schrems II ruling (§185) “*the limitations on the protection of personal data arising from the domestic law of the United States on the access and use by US public authorities of such data transferred from the European Union to the United States, which the Commission assessed in the Privacy Shield Decision, are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required, under EU law, by the second sentence of Article 52(1) of the Charter*”. Therefore transfers to the USA, without supplementary measures taken by the public bodies, as Controllers, may take place in breach of the GDPR and the Controllers may, consequently, not be able to demonstrate compliance, according to the accountability principle.

#### **6.4. Differences between stakeholders:**

- Only one public body responded that no transfers of personal data take place, and, regarding telemetry/diagnostic data, especially in relation to Office 365, the telemetry feature is no longer provided by the CSP (Microsoft), therefore no transmission of such data takes place.

#### **6.5. Potential solutions to this issue by the SA or the stakeholders:**

- Controllers should assess and implement appropriate specific supplementary measures in order to frame possible transfers to third countries, based on their needs and processing characteristics. If such measures are not found sufficient, the public bodies should consider choosing another CSP. In case a breach is found, the SA may take action through corrective measures (orders or administrative fines).

### **Part III – Actions by the SA**

1. **Have you taken action (i.e. fact-finding exercises, informal contact, prior consultation, investigation) towards any of the stakeholders concerning the use of cloud-based services prior to launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**
  - Our SA has not taken any action towards any of the stakeholders prior to the coordinated action.
2. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (E.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**
  - As this is an ongoing case, further investigation is required on the issues identified in the above analysis, particularly regarding the role of the parties involved in the processing and their obligations under the GDPR, the ability of the stakeholders to meaningfully negotiate with the CPS on the terms of the contract and the selection of the sub-contractors as well as the conditions under which international transfers take place.

- In this phase, the Authority plans to send letters to the parties involved in order to collect additional information, documentation and clarification with the goal to resolve the identified issues and publish recommendations and instructions to the public bodies.
- Then, based on the further results and evidence collected, the Authority will redefine its plan of action without excluding any corrective measures.

#### **Part IV – Other**

1. **What is your general impression of the levels of awareness and compliance of the stakeholders you consulted concerning the use of cloud?**
  - In general, the level of awareness can be considered as relative low at the beginning of the coordinated action. However, some public bodies reported that, in order to provide answers to the questionnaire, they started gathering information and considering issues that they had not examined thoroughly before. This already indicates an increase in the awareness level of public bodies, which the Authority intends to strengthen with its further actions.
2. **Are there any other issues or topics that you would like to flag?**
3. **Are there any leading practices of the stakeholders you have contacted that you would like to share?**

## Part I - Statistics

1. **How many stakeholders have you contacted within the following categories?**

- 9 institutions Ministry of the central government
- 3 institutions Independent public body of the central government

2. **How many stakeholders have you contacted within the following sectors?**

- 1 institution: Agriculture
- 1 institution: Economic affairs
- 1 institution: Finance
- 1 institution: Health
- 2 institutions: Infrastructure
- 2 institutions: Justice
- 1 institution: Tax
- Other, 1 institution: Research
- Other, 1 institution: Culture
- Other, 1 institution: Governments coordinator

3. **If you have contacted a buyer, for which sectors does this buyer provides its services:**

- Not applicable.

4. **If you have contacted a buyer, and if you have this information, please specify the number of stakeholders this buyer provides services for:**

- Not applicable.

5. **What was the initial procedural framework of your action?**

- Fact-finding + determining follow-up action based on the results.

6. **How many stakeholders indicated that they use CSPs or are planning to do so in the near future (end of 2022)?**

- A total of twelve controllers were contacted. Eleven of them were already using CSPs and just one declares that has its own cloud infrastructure.

7. **Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?**

- 11 institutions for Internal organisation (office suites, internal communication, HR, etc.).
- 7 institutions for Exercise of public functions (services to citizens, processing citizen's data, etc.).

8. **For the following commonly identified sectors, please specify if any hyper-scalers<sup>33</sup> are involved (if so please name them) either because they provide the services themselves or because the services are using the infrastructures of these hyper-scalers.**

- 1 institution – (Microsoft 365) - Finance
- 1 institution- (Amazon AWS) - Tax

---

<sup>33</sup> Hyper-scalers provide cloud services at scale. It refers usually to the big cloud providers (Google, AWS, Microsoft ...) on which other services may also depend

**9. How many stakeholders took the following actions prior to- or during the acquisition of a CSP?**

- Perform a DPIA. **None.**
- Does the DPIA analyse transfers in detail (sometimes called DTIA). **None.**
- Contact the DPO for advice. **3 institutions.**
- Perform a general risk analysis. **None.**
- Contact the SA for advice. **None.**

**10. How many stakeholders (including buyers) take the following actions during the use of the CSP?**

- Monitoring technical and organisational measures to ensure compliance: **None**
- In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g. Schrems II): **None of the institutions declares transfers of personal data.**
- Regular risk assessments: **None.**

## Part II - Substantive issues

**1. DPO involvement and position**

- Most of the controllers might have not consulted the DPO when they decided to hire the services of a CSP, which besides the lack of advice to data controller might involve difficulties with the position of the DPD.
- Provisions of articles 35 and 38. Although, in some cases, it is possible that the contractual terms had been achieved prior to the publication of the RGPD which, initially, would imply that these institutions, at that moment, had not designated the DPO given that in Spain the obligation to have a DPO materializes in 2016 with the publication of the RGPD.
- Most of the controllers explain that they did not consult the DPO when they decided to hire the services of a CSP since they understood that security measures were enough.
- On the other side, none of the controllers that have consulted the DPO did not receive a negative response regarding the hiring of the CSP, which might also involve some misunderstanding on the side of the DPO as far as security as a principle of personal data protection and not as the only principle to consider.

**What are the differences that you have encountered between stakeholders in your Member State?**

- None. Most of the bodies did not consult the DPO.

**What are the solutions to this issue? Please describe if these solutions are already implemented or potential, and whether this solution is provided by the SA or the stakeholders.**

- Working on guidelines for data controllers and data processors within GDPR regulation, according to EDPB final report and recommendations, for instance, updating with these recommendations the Spanish guidelines for controllers and processors on the context of cloud computing.

**2. Risk Assessment**

- None of the entities has carried out a risk assessment when making this contract.
- Risk assessment for the rights and freedoms of citizens might have been understood as the risk assessment to set up security technical and organizational measures that would answer to GDPR article 32, which might mean a reduction of personal data protection to the mere existence of

security measures that could have been established without adequate assessment of risks referred to in recital 83, an issue that has been addressed in the guide to "Risk management and impact assessment in the processing of personal data of the AEPD".

- It seems that the reason might be a misunderstanding of the obligation to carry out a risk assessment according to the GDPR.
- None as none of the controllers has carried out a GDPR risk assessment.

**What are the solutions to this issue? Please describe if these solutions are already implemented or potential, and whether this solution is provided by the SA or the stakeholders.**

- Working on guidelines for data controllers and data processors within GDPR regulation, according to EDPB final report and recommendations, for instance, updating with these recommendations the Spanish guidelines for controllers and processors on the context of cloud computing.

### **3. Realization of DPIA**

- In line with issue number 2, most of the controllers consulted have not carried out a DPIA of the services implemented in CSP.
- Article 35 of the GDPR. This should be an aspect included by CSP as a service by default characteristic at least within the context and scope they know.
- The fact that the CSP is certified according to the Spanish National Security Scheme was understood by most of the controllers and processors as more than enough for hiring the CSP services, so they did not consider carrying out a DPIA.
- Again, risk assessment for the rights and freedoms of citizens is reduced to providing security measures.
- There are no major differences, as most of the controllers consulted have not carried out a DPIA. One of the controllers has pointed out three CSP contracts in which the corresponding DPIA has been carried out but without doing the same in the rest of its contracts.
- Some of those who have not performed the DPIA do not respond to the reason why they do not perform the DPIA.
- Working on guidelines for data controllers and data processors within GDPR regulation, according to EDPB final report and recommendations, for instance, updating with these recommendations the Spanish guidelines for controllers and processors on the context of cloud computing.

### **4. D. Hiring the CSP and Contract Negotiation**

- It seems that for some of the controllers the contract for hiring the CSP does not fully cover some key points of compliance with the GDPR, as it is the processor relationship.
- Article 28.3 states that the details of the processing by the processor shall be governed by a contract or other legal act and only a few bodies include this relationship in the contract.
- In the absence of a detailed analysis of this contractual relationship, it is unknown whether this is up to the so called "adhesion contracts" of the CSP service or whether the controller has the capacity to modify the contractual clauses to require the CSP to comply with the requirements of the GDPR.

- The main chosen CSP by almost all controllers is Microsoft with its Office 365 and Azure products. Followed by Amazon Web Services (AWS), which has been chosen by some entities.
- Regarding the obligations of the processor, only some bodies include them in the contract, and some bodies refer to the CSP being certified according to the Spanish National Security Scheme. Once again, GDPR and the obligations required by Article 28 might be reduced to the existence of a security framework regardless of the implicit risk that the processing could imply for the rights and freedoms of natural persons.
- Some of the controllers seem that they did not have any chance to negotiate the terms of the contract in order to reduce the possible risks related to the processing of personal data, which could reveal the existence of so-called "adhesion contracts" that come to be previously defined by the CSP without the possibility of modification by the data controller, though this cannot be determined from the scope of this report.
- The scope of the present action does not allow for a detailed analysis of the contracts between the institutions and the CSP, it is not possible to determine these differences.
- Besides working on guidelines for data controllers and data processors within GDPR regulation, according to EDPB final report and recommendations, for instance, updating with these recommendations the Spanish guidelines for controllers and processors on the context of cloud computing. We would suggest working based on the provisions of article 28 paragraphs 7 and 8 providing the market with contractual models according to GDPR provisions.

##### **5. E. Audit and monitoring actions of controllers**

- Monitoring of implementation of technical and organizational measures by the CSPs.
- It has only been identified monitoring of technical and organizational measures to ensure security of information and the continuity of the business operations of the institutions, that is, monitoring actions of CSPs in line with the certification procedures involved in each case. It is not known whether this is also the case when dealing with GDPR.
- As a verification measure, controllers generally verify that the CSP is certified according to the Spanish National Security Scheme.
- It is not known within the context of this report, whether controllers go beyond verifying security measures and do not verify other measures such as, for instance, data protection measures by design or by default, concrete application of the principle of minimization by the CSP or even security measures specifically aimed for managing rights and freedoms risks. A deeper and specific analysis based on each personal data processing should be required.

##### **What are differences that you have encountered between stakeholders in your Member State?**

- None of all the controllers monitors the implementation of technical and organizational measures.

##### **What are solutions to this issue? Please describe if these solutions are already implemented or potential, and whether this solution is provided by the SA or the stakeholders.**

- Once again, working on guidelines for data controllers and data processors within GDPR regulation, according to EDPB final report and recommendations, for instance, updating with these recommendations the Spanish guidelines for controllers and processors on the context of cloud computing.

### **Part III - Actions by the SA**

1. Have you taken action (i.e. fact-finding exercises, informal contact, prior consultation, investigation) towards any of the controllers concerning the use of cloud-based services prior to launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the controller, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).
  - The AEPD did not take actions towards any of the questioned institutions prior to the coordinated action.
2. What action(s) are you planning to undertake based on the results of this coordinated action, if any? (E.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing).
  - It is up to the general conclusions and recommendations of the final EDPB report.

### **Part IV - Other**

1. What is your general impression of the levels of awareness and compliance of the stakeholders you consulted concerning the use of cloud?
  - It seems that there is not awareness at all about issues as data transfers, CSP processing telemetry data or foreign countries governments disclosing the data.
2. Are there any other issues or topics that you would like to flag?
  - No
3. Are there any leading practices of the stakeholders you have contacted that you would like to share?
  - One of the consulted controllers have declared that for security reasons they have established in their internal regulations the strict control of all sensitive information, both from the point of view of personal data protection and information security, and according to this they do not use any CSP. For its own business operation, this controller has its own private cloud, managed by itself and without hiring any external service.

# FI SA

The Office of the Data Protection Ombudsman

## Part I – Statistics

### 1. How many stakeholders have you contacted within the following categories?

- Ministry of the central government
- Independent public body of the central government: **2 stakeholders**
- Buyer for the central government: **1 stakeholder**
- Publicly-owned company acting as a processor for several central public bodies
- Ministry of the regional government
- Independent public body of the regional government
- Buyer for the regional government
- Publicly-owned company acting as a processor for several regional public bodies
- Other, please specify

### 2. How many stakeholders have you contacted within the following sectors?

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government: **1 stakeholder**
- Economic affairs
- Education
- Finance
- Health
- Infrastructure
- Employment
- Justice
- Tax: **1 stakeholder**
- Other, please specify: **Government ICT centre - 1 stakeholder**

### 3. If you have contacted a buyer, for which sectors does this buyer provides its services:

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government
- Economic affairs
- Education
- Finance
- Health
- Infrastructure
- Employment
- Justice
- Tax
- No specific sector: **1 stakeholder - All government agencies and institutions, also including government-owned corporations, other public authorities, bodies governed by public law, the parliament, funds that are not within the scope of the government budget and companies or organisations with public administration or service responsibilities.**
- Other, please specify

**4. If you have contacted a buyer, and if you have this information, please specify the number of stakeholders this buyer provides services for:**

- This information was not requested from the stakeholders the FI SA contacted.

**5. What was the initial procedural framework of your action?**

- Fact finding
- Fact finding + determining follow-up action based on the results
- New investigation<sup>34</sup>
- Ongoing investigation

**6. How many stakeholders indicated that they use CSPs or are planning to do so in the near future (end of 2022)?**

- All 3 stakeholders

**7. Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?**

- Internal organisation (office suites, internal communication, HR, etc.): **all 3 stakeholders**
- Exercise of public functions (services to citizens, processing citizen's data, etc.): **all 3 stakeholders**

**8. For the following commonly identified sectors, please specify if any hyper-scalers<sup>35</sup> are involved (if so please name them) either because they provide the services themselves or because the services are using the infrastructures of these hyper-scalers.**

- Health
- Finance
- Tax – **Microsoft**
- Education
- Central buyers or providers of IT services - **AWS, Microsoft**

**9. How many stakeholders took the following actions prior to- or during the acquisition of a CSP?**

- Perform a DPIA: **2 stakeholders**
- Does the DPIA analyse transfers in details (sometimes called DTIA): **2 stakeholders**
- Contact the DPO for advice: **all 3 stakeholders**
- Perform a general risk analysis: **all 3 stakeholders**
- Contact the SA for advice

**10. How many stakeholders (including buyers) take the following actions during the use of the CSP?**

- Monitoring technical and organisational measures to ensure compliance: **all 3 stakeholders**
- In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g., Schrems II): **2 stakeholders**
- Regular risk assessments: **all 3 stakeholders**

## **Part II – Substantive issues**

---

<sup>34</sup> making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred

<sup>35</sup> Hyper-scalers provide cloud services at scale. It refers usually to the big cloud providers (Google, AWS, Microsoft ...) on which other services may also depend

## **1. At pre-contractual phase**

### **1.1. Other stakeholders (controllers) cannot effectively affect the decisions made by the central buyer regarding the use of CSPs (incl. transfers to third countries)**

- Relates to Articles 24, 28, 44 and 46 GDPR.
- One stakeholder stated that it cannot fully ensure the lawfulness of the processing performed by the sub-processors. This stakeholder has also stated that they only have limited knowledge regarding the sub-processors used by the CSP. The contract between the other stakeholders (customers) and the central buyer states that personal data may only be accessed and processed within the EEA unless there is a prior written consent of the controller. Regardless of this, the central buyer seems to use sub-processors that transfer personal data to third countries. It should be noted, that for the stakeholders the use of the central buyer is mandatory under Finnish legislation.
- The controller should have power regarding the use of sub-processors as described in Article 28 GDPR and the central buyer should only use sub-processors which process data within the EEA unless otherwise agreed upon.
- There have been some inaccuracies in the contract between the central buyer and Microsoft regarding roles. In 2021, the central buyer added an additional agreement to the contract with Microsoft where it was clarified that other stakeholders act as controllers. This additional agreement mainly clarifies the roles between the central buyer and the stakeholders (its customers).

## **2. In the contract with the CSP**

### **2.1. CSPs are processing personal data for their own purposes**

- Relates to Articles 28(1) and 28(10) GDPR.
- Stakeholders cannot ensure compliance with the GDPR since they cannot change the CSP even if the (sub-) processor would process personal data against the GDPR and/or the stakeholder's instructions.

### **2.2. Stakeholders have restricted negotiating power in relation to contracts with the CSPs**

- Relates to Articles 28(1), 28(3) and 28(10) GDPR
- The contract between stakeholders and AWS/Microsoft is mainly predetermined by AWS/Microsoft.

### **2.3. Stakeholders have no influence on the sub-processors used by AWS/Microsoft. Not all the sub-processors have been identified.**

- Relates to Article 28(2) GDPR.
- The central buyer has stated that AWS/Microsoft informs its customers about changes made to the sub-processors in its newsletter/on its website. The central buyer can object to the use of such sub-processors only by terminating the contract.

## **3. On International transfers and access by foreign public authorities**

### **3.1. No transfer impact assessment (TIA) has been made regarding the use of CSPs**

- Relates to Articles 24, 44 and 46 GDPR.
- One stakeholder has performed its own TIA relating to Microsoft and at the time of the survey, this stakeholder was working on its own TIA relating to AWS. Another stakeholder has not performed a TIA since it is of the opinion that there are no data transfers outside the EU/EEA.

### **3.2. Stakeholders have not been able to identify appropriate and effective supplementary measures.**

- Relates to Articles 44 and 46 GDPR.

- This matter has been an issue for all three stakeholders because there are no appropriate safeguards to ensure the required level of protection when transferring personal data to third countries. It seems that the central buyer has not been able to process personal data in accordance with all of the controller's (customer's) instructions.
- One stakeholder has identified technical supplementary measures in most cases (encryption, pseudonymization, Customer Lockbox) but their effectiveness is not always clear (e.g., in some cases the encryption keys are governed by the CSP and device and user data is possibly transferred to the U.S.). The stakeholder in question states that the risk for data subjects has been estimated to be low, as the transferred information is restricted and includes employee names and emails, which are nationally regarded as public information. However, the supplementary measures that two of the stakeholders have adopted seem inadequate and e.g., in relation to support and maintenance tasks no supplementary measures have been identified.

### **3.3. Risk of access by foreign public authorities**

- Relates to Article 6 and Chapter V GDPR.
- One stakeholder has identified that foreign public authorities could have access to the personal data under third country legislation. However, the stakeholders have not been notified of any request for disclosure of personal data. Another stakeholder thinks it is unlikely that public authorities in the U.S. would try getting access to the data via intelligence gathering, as there are many international agreements related to the information it processes that already offer the U.S. authorities the possibility to get access to relevant information in a more efficient way.

## **Part III – Actions by the SA**

1. Have you taken action (i.e., fact finding exercises, informal contact, prior consultation, investigation) towards any of the stakeholders concerning the use of cloud based services prior to launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g., letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).
  - No.
2. What action(s) are you planning to undertake based on the results of this coordinated action, if any? (e.g., letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)
  - The FI SA has not yet decided what actions will be taken in this matter. The investigation is still ongoing.
  - However, the FI SA stresses that in the Schrems II judgment (C-311/18), the Court clearly stated that if a supervisory authority takes the view, following an investigation, that a data subject whose personal data have been transferred to a third country is not afforded an adequate level of protection in that country, it is required, under EU law, to take appropriate action in order to remedy any findings of inadequacy, irrespective of the reason for, or nature of, that inadequacy. Therefore, if the FI SA takes the view that stakeholders have infringed Chapter V of the GDPR, the FI SA must use its corrective powers listed in Article 58(2) of the GDPR.
  - It should be noted that an administrative fine cannot be issued to public authorities in Finland.

## **Part IV – Other**

**1. What is your general impression of the levels of awareness and compliance of the stakeholders you consulted concerning the use of cloud?**

- The general level of awareness related to the data protection issues when using CSPs seems satisfactory, but several concerns remain.
- The first stakeholder is aware of the risks concerning the use of CSPs. It has stated that there is a conflict, which arises from the fact that the contract terms of CSPs do not meet the requirements of the GDPR in all respects. The second stakeholder has taken many measures (risk assessments, DPIA, TIA, cooperation and information sharing with stakeholders and international colleagues) in trying to ensure its compliance with the GDPR and Chapter V. However, several issues remain as described above. The third stakeholder points out that it has little power in ensuring GDPR compliance due to the central buyer being responsible for the acquisition of CSPs. This stakeholder emphasizes its contract with the central buyer and the responsibilities of the central buyer as a processor and the fact that according to their agreement personal data should only be processed and accessed within the EEA, unless prior written consent is given by the stakeholder.
- Stakeholders also refer to the constantly changing legal environment, partly contradictory case law in different Member States and lack of guidance from SAs as further challenges.

**2. Are there any other issues or topics that you would like to flag?**

**3. Are there any leading practices of the stakeholders you have contacted that you would like to share?**

# IS SA

Icelandic Supervisory Authority - Persónuvernd

## Part I – Statistics

### 1. How many stakeholders have you contacted within the following categories?

- Ministry of the central government: **None**
- Independent public body of the central government: **None**
- Buyer for the central government: **None**
- Publicly-owned company acting as a processor for several central public bodies: **None**
- Ministry of the regional government: **None**
- Independent public body of the regional government: **None**
- Buyer for the regional government: **Six municipalities**
- Publicly-owned company acting as a processor for several regional public bodies: **None**
- Other, please specify: **Not relevant**

### 2. How many stakeholders have you contacted within the following sectors?

- Agriculture: **None**
- Defence: **None**
- Digitalisation of the Public Administration/e-Government: **None**
- Economic affairs: **None**
- Education: **Six**
- Finance: **None**
- Health: **None**
- Infrastructure: **None**
- Employment: **None**
- Justice: **None**
- Tax: **None**
- Other, please specify: **Not relevant**

### 3. If you have contacted a buyer, for which sectors does this buyer provides its services:

- Education

### 4. If you have contacted a buyer, and if you have this information, please specify the number of stakeholders this buyer provides services for:

- Municipality of Akureyri: 10 elementary schools
- Municipality of Garðabær: 6 elementary schools
- Municipality of Hafnarfjörður: 9 elementary schools
- Municipality of Kópavogur: 9 elementary schools
- Municipality of Reykjanesbær: 7 elementary schools
- Municipality of Reykjavík: 39 elementary schools

### 5. What was the initial procedural framework of your action?

- New investigation in the form of audits.

### 6. How many stakeholders indicated that they use CSPs or are planning to do so in the near future (end of 2022)?

- All six. However, the scope of the investigation has been limited to the use of cloud services provided by Google LLC, and additionally in the case the municipality of Kópavogur, Seesaw, for

the processing of personal data regarding students at elementary schools (age 6-16). However, the DPA's investigation of the municipality of Akureyri has been terminated, as it was not found to be a controller, under article 4(7) of Regulation (EU) 2016/679 of the data processing subject to the scope of the investigation. This was due to the fact that the municipality does not decide whether its elementary schools are to use CSPs, and if so, which ones. Rather individual elementary schools, operated by the municipality, decide individually whether they introduce cloud-based services in their teachings and which CSPs are appropriate for that purpose.<sup>36</sup>

**7. Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?**

- Internal organisation (office suites, internal communication, HR, etc.): **Not relevant in the light of the scope of the investigation, as discussed under question 6.**
- Exercise of public functions (services to citizens, processing citizen's data, etc.): **Five**

**8. For the following commonly identified sectors, please specify if any hyper-scalers<sup>37</sup> are involved (if so please name them) either because they provide the services themselves or because the services are using the infrastructures of these hyper-scalers**

- Education / Google LLC

**9. How many stakeholders took the following actions prior to- or during the acquisition of a CSP?**

- **Perform a DPIA:**

**In relation to services provided by Google:**

- DPIAs in relation to the use of Google's cloud-based services have been presented by three municipalities. However, two municipalities are of the view that they were not obliged to perform DPIAs in relation to Google services as their use was initiated before the Icelandic Data Protection Act no. 90/2018 (which incorporates Regulation (EU) 2016/679 to Icelandic Law) came into force. Yet, both municipalities have informed the SA that DPIAs are currently being performed in relation to the services.

**In relation to services provided by Seesaw:**

- DPIA in relation to the use of Seesaw's cloud-based services has been presented by the only municipality that is under investigation for the use of the CSP.

- **Does the DPIA analyse transfers in details (sometimes called DTIA):**

**In relation to services provided by Google:**

- DPIAs of two municipalities contain provisions, to a varying degree of detail, on transfer of personal data to third countries.

**In relation to services provided by Seesaw:**

- DPIA contains a general provision on the transfer of personal data to the United States.

---

<sup>36</sup> The SA takes notice of this scope when providing answers to following questions in this report. As a result, the replies below reflect only the actions and inactions of the municipalities that are currently under investigation by the SA in relation to their use of services of Google and Seesaw in the field of education. In contrast, information related to the use of *other* CSPs by the municipalities that are under investigation are disregarded. Similarly, information regarding the use of all CSPs by the municipality of Akureyri are disregarded.

<sup>37</sup> Hyper-scalers provide cloud services at scale. It refers usually to the big cloud providers (Google, AWS, Microsoft ...) on which other services may also depend

- **Contact the DPO for advice**

**In relation to services provided by Google:**

- It appears that DPOs have been contacted for advice to some degree by four to five municipalities (uncertainty in the light of the discussion under the next bullet) in relation to their use of cloud-based services provided by Google, either prior, during or after the introduction of the services. However, it must be noted that some of the municipalities did not employ DPOs when the use of the services was initiated.

**In relation to services provided by Seesaw:**

- It appears that the DPO was not contacted in relation to the introduction of the service in question. However, in the replies of the municipality that are not software-specific, it holds that the DPO is contacted in later stages in the relation to introduction of cloud-based services in general, e.g. for review of DPOs and risk assessments. Yet, the municipality has admitted that the DPO's advice to seize the use of Seesaw, given after the SA's decision discussed under part III, was not adhered.

- **Perform a general risk analysis**

All five municipalities appear to perform a general risk analysis to some degree in relation to cloud-based services. It should also be highlighted that the Icelandic Association of Local Authorities has performed a general risk analysis for multiple software programs in the field of education.

- **Contact the SA for advice**

A survey of the SA's case registry indicates that two of the municipalities, that are under the current investigation, made a joint request for an information meeting with the authority, regarding the use of CSPs, including cloud-based services provided by Google in the field of education. The request was granted by the authority. According to the meeting minutes, the municipalities were provided with some general information on the matter.

**10. How many stakeholders (including buyers) take the following actions during the use of the CSP?**

- Monitoring technical and organisational measures to ensure compliance: **Two municipalities monitor, to some degree, technical and organisational measures to ensure compliance. Three municipalities do not monitor technical and organisational measures to ensure compliance.**
- In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g. Schrems II): **One municipality has adopted technical and organisational measures, including supplementary measures, where needed, in the case of transfers. Four municipalities do not appear to have adopted such measures. None of the municipalities monitor changes in the regulatory landscape in a systematic manner, although four of them perform checks if need arises (incident-based approach).**
- Regular risk assessments: **None of the municipalities appears to perform systematic risk assessment.**

### **Part III – Actions by the SA**

**1. Have you taken action (i.e. fact-finding exercises, informal contact, prior consultation, investigation) towards any of the stakeholders concerning the use of cloud-based services prior to launching the coordinated action? Please describe the action you have taken and the**

**outcome of this action (e.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

- In April 2021, the Icelandic Supervisory Authority (SA) was notified that one of Reykjavík's elementary schools was obtaining consent from parents for processing of personal data of students using the Seesaw educational system, which is an American cloud-based service. The Icelandic SA subsequently examined on its own initiative the use of the Seesaw educational system by elementary schools in Reykjavík.
- On December 20, 2021, the Icelandic SA concluded that the municipality of Reykjavík had breached various provisions of the GDPR using Seesaw. Following that decision, the Icelandic SA examined whether there were grounds for imposing an administrative fine. In its decision on May 3, the Icelandic SA concluded that the municipality of Reykjavík was to pay a 5.000.000 ISK fine.
- Key findings of the Icelandic SA's former decision were i.a. that the processing agreement between Reykjavík and Seesaw was insufficient, that the municipality could not demonstrate a specified, explicit and legitimate purpose for the processing in question, which was therefore considered unlawful, that the processing was neither fair nor transparent, that the principles of data minimisation and storage limitations were not implemented nor data protection by design and by default, taking into consideration the amount of data collected, the extent of their processing, the period of their storage and their accessibility, that the data protection impact assessment did not meet the minimum requirements, that the municipality did not demonstrate that it had ensured appropriate security of the personal data in question and that the data was being transferred to the United States without appropriate safeguards.
- The Icelandic SA furthermore concluded that all processing in the Seesaw educational system should be seized and students' data deleted after being retrieved, if applicable, to be stored within each school.
- Key findings of the latter decision were that, due to all the above and taking into consideration i.a. that the infringements concerned the personal data of children and that it was considered likely that special categories of data and other sensitive information were being processed; but also that no damage appeared to have been caused by the violations, that there was no indication that Seesaw's general information security was not adequate and that the municipality co-operated with the SA in a clear and concise manner, a 5.000.000 ISK administrative fine was imposed on the municipality of Reykjavík.
- The SA's decision was to impose an administrative fine on Reykjavik of a fee of appr. 35.768 EUR.

**2. What action(s) are you planning to undertake based on the results of this coordinated action, if any? (E.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

- The Icelandic SA has not determined the appropriate course of actions based on the coordinated enforcement actions, given the fact that no decision on the legality of substantive issues has been rendered. In this context, it must also be stressed that according to article 38(3) of the Icelandic Data Protection Act no. 90/2018, the SA's board is responsible for making any major material or policy-making decisions in matters that are being processed by the authority, including the imposition of administrative fines.

## **Part IV – Other**

**1. What is your general impression of the levels of awareness and compliance of the stakeholders you consulted concerning the use of cloud?**

- The SA is of the view that all five municipalities, currently under investigation, have a rudimentary awareness regarding the use of cloud-based services and data protection. However, in the light of the discussion under question 2 in part III, the SA does not view it as timely to signal its impression on the municipalities' compliance to the legal framework of data protection.

**2. Are there any leading practices of the stakeholders you have contacted that you would like to share?**

- Not relevant.

# IT SA

Italian SA – Garante per la protezione dei dati personali

## Part I – Statistics

### 1. How many stakeholders have you contacted within the following categories?

- Ministry of the central government: 1
- Independent public body of the central government
- Buyer for the central government
- Publicly-owned company acting as a processor for several central public bodies: 2
- Ministry of the regional government
- Independent public body of the regional government
- Buyer for the regional government
- Publicly-owned company acting as a processor for several regional public bodies: 2
- Other, please specify

### 2. How many stakeholders have you contacted within the following sectors?

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government: X
- Economic affairs
- Education
- Finance
- Health
- Infrastructure
- Employment
- Justice
- Tax
- Other, please specify: **By addressing our action to publicly-owned companies acting as processors for several public bodies (at both national and regional level), many stakeholders in different sectors of the public administration could be involved (indirectly) including the sectors of Digitalisation of public administration, Finance, Health and Social security, Tax, Infrastructures, Employment, Justice.**

### 3. If you have contacted a buyer, for which sectors does this buyer provides its services:

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government
- Economic affairs
- Education
- Finance
- Health
- Infrastructure
- Employment
- Justice
- Tax
- No specific sector
- Other, please specify: N/A

**4. If you have contacted a buyer, and if you have this information, please specify the number of stakeholders this buyer provides services for:**

- N/A

**5. What was the initial procedural framework of your action?**

- Fact finding
- Fact finding + determining follow-up action based on the results: **X**
- New investigation<sup>38</sup>: **X**
- Ongoing investigation: **X**

**6. How many stakeholders indicated that they use CSPs or are planning to do so in the near future (end of 2022)?**

- All stakeholders are using or planning to use CSPs by the end of 2022 for some services

**7. Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?**

- Internal organisation (office suites, internal communication, HR, etc.): **All of them use (different) cloud services for their internal organisation**
- Exercise of public functions (services to citizens, processing citizen's data, etc.): **All of them use CSPs (and plan to use them) for the exercise of public functions**

**8. For the following commonly identified sectors, please specify if any hyper-scalers<sup>39</sup> are involved (if so please name them) either because they provide the services themselves or because the services are using the infrastructures of these hyper-scalers**

- Health
- Finance
- Tax
- Education
- Central buyers or providers of IT services
- In most cases, the main hyper-scalers are involved both because they provide the services and because their infrastructures are used

**9. How many stakeholders took the following actions prior to- or during the acquisition of a CSP?**

- Perform a DPIA: **2**
- Does the DPIA analyse transfers in details (sometimes called DTIA): **1**
- Contact the DPO for advice: **2**
- Perform a general risk analysis: **1**
- Contact the SA for advice: **1**

**10. How many stakeholders (including buyers) take the following actions during the use of the CSP?**

- Monitoring technical and organisational measures to ensure compliance: **3**
- In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g. Schrems II): **0**

---

<sup>38</sup> making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred

<sup>39</sup> Hyper-scalers provide cloud services at scale. It refers usually to the big cloud providers (Google, AWS, Microsoft ...) on which other services may also depend

- Regular risk assessments: 2

## Part II – Substantive issues

### 1. At pre-contractual phase

#### 1.1. Role of the resellers from a data protection point of view and responsibilities in case of inconsistency between the public procurement and the contract signed with the CSP.

- One of the main issues identified in relation to the pre-contractual phase is related to the role of the resellers of cloud services. Usually, the cloud services are not directly negotiated with the CSPs (in many cases hyper-scalers) but via Italian companies acting as resellers and the exact role of these resellers is not always clear from a data protection point of view. In some cases, for example, even where the resellers do not play any active role in processing personal data in relation to the provision of the cloud services, they have been nevertheless designated as data processors.
- GDPR provision concerned: Article 28 and, in particular, the way in which obligations under art. 28(3) GDPR may be complied with in practice.
- This issue has been dealt with in different ways. In some cases, resellers are considered to be solution providers that play only an intermediation role for the purchase and payment of services, while, with regard to the processing of personal data, the hyper-scaler has a direct relationship with the public body (which includes the public authority as the controller and the publicly-owned company acting as processor for a given public authority, all of them being referred to hereinafter as ‘PA’) which has designated the CSP as data processor/sub-processor (so called “End Customer Account Model”). This model provides for a direct relationship between the PA and the hyper-scaler for the access to and use of cloud services, thus ensuring – among the other things – the continuity of the services even following termination of the contract with the reseller.
- In other cases, the relationship between the PA and the hyper-scalers is mediated by the resellers, which are designated as data processors even though they do not process personal data in relation to the cloud services provided. The Data Processing Agreement/Addendum is undersigned between the reseller and the CSP, and the PA has no direct relationship with the CSP. Indeed, on the assumption of the absence of a direct contractual relationship between the PA and the CSP, CSPs require the PA to interact with the reseller and commit all compliance obligations to the reseller, whilst in practice all services and processing activities are carried out directly by the CSPs. In these cases, it is difficult for the PA to provide full instructions to the actual processor and to assess its compliance: CSPs often refuse to accept to negotiate specific clauses in the contracts with the PA and to receive direct instructions from them. These difficulties seem to be compounded by the widespread use of model contracts in which it is clearly stated that they are to be considered as Customer’s documented instructions for the processing of Personal Data and which may only be adhered to without any possibility to negotiate specific amendments (see issues related to difficult negotiations).
- In addition, some stakeholders have complained that there are cases where they have provided the reseller acting as a processor with specific instructions (e.g. to provide information on data breaches within a specific timeframe), but the same instructions have not been imposed on the CSPs because of the reduced ability to negotiate clauses that, as mentioned before, are already contained in the contract/data processing addendum prepared by the CSP.

### 2. In the contract with the CSP

## **2.1. Difficult negotiations and unilateral amendments**

- In all investigated cases, it was difficult for the public administration to negotiate a bespoke contract, considering that hyper-scalers offers standard contracts they may unilaterally modify.
- GDPR provision concerned: Article 5(2) and Article 28 GDPR.
- Stakeholders generally complained about the main difficulties encountered in this context and in particular called the attention to: 1. the difficulties for the PA to negotiate aspects relating to the protection of personal data processed by the CSP on its behalf, pending the reseller's intermediation in the aforementioned contractual relationship (see previous issue relating to the resellers' role) and considering that the resale contract is not different from the contract for the provision of the service; 2. The imbalance in negotiation with the main CSPs on the market, which make use of predefined service terms, in relation to which the PA has often not been able to obtain all the changes required; 3. How service terms are amended and how they are notified. The notification rules are the same for any kind of contractual amendment; however, according to the stakeholders, these rules should be different (e.g. in the timing envisaged) by having regard to the different characteristics and impact of the amendments on the processing of personal data.
- It is a widespread impression among the stakeholders that when various public bodies try to cooperate in negotiating with the CSPs or if one of them negotiates the same services on behalf of several public bodies, the imbalance in negotiation seems to be reduced and this is the reason why few of them already tried in the past to have talks with other entities at national level (including when possible the central buyers) at least in order to identify and discuss the main criticalities of the contracts for the services provided by the main CSPs and possible ways of addressing them. However, in the absence of coordinated actions, each PA has to independently negotiate conditions or settings with the CSP and this undermines their power.
- In a few cases, the stakeholders have initiated talks with the CSP aimed at negotiating some changes to the current standard contract in place. These discussions have made it possible to clarify certain aspects of contractual clauses contained in the DPA, but have not led generally to the negotiation of specific conditions with some minimal exceptions. However, following some requests for clarification or modification made by the stakeholders, the CSP has amended its standard documentation.

## **2.2. Designation of sub-processors**

- Usually, the CSPs engage sub-processors on the basis of general written authorisations by the PA which are given the opportunity to object to any change to the list. However, PA are often informed about the sub-processors involved in routine service provision or support services by means of webpages in which they are listed and only in some cases (e.g. if the public authorities have indicated contact details, such as an email address) are they informed directly about amendments to such list and therefore about changes of sub-processors. In most cases, failure to object to new sub-processors is interpreted as an authorisation and if the PA objects to a sub-processor, the usual contractual recourse is to terminate its subscription to the given service. If the service is part of a suite, the PA must terminate its subscription to the entire suite. The other option, especially for sub-processors providing support services, is to limit as far as possible both the use of the service in question and the data shared in connection with a support case. All of this could result in the loss of potentially business critical services and have implications for the controller's ability to deliver public services in a timely manner and, as a result, risks undermining the right to object to changes of sub-processors envisaged by Article 28(2) GDPR in case of a general authorisation.

- GDPR provision concerned: Article 28 (2) and 28(4).
- Difficulties have been highlighted by PA in negotiating different rules on the identification/changes of sub-processors since most CSPs seem not to be inclined to change their model considering that, in many cases, it would not be possible for them to provide services in a different way.
- Furthermore, generally, there is no specific list of the sub-processors that are actually used by the CSP to provide the required services to the relevant PA. The list provided is a general one and, even in the course of or after the investigations, it was difficult for the PA to be provided with information about the sub-processor involved in the processing activities related to the services provided to them - in spite of the need for the controller to be in effective control of the chain of entities processing personal data on its behalf. Only in a few cases, upon specific request, has the public authority been provided with the list of the specific sub-processors.
- Reference should be made to a case where, in order to try to ensure that the controller retained a sufficient level of control over the selection of new sub-processors, a contractual amendment was implemented so as to grant the controller a meaningful right to review the change of the list of relevant sub-processors and to transmit reasoned objections within a predefined period. In this event, the CSP may obtain the termination of the contractual relationship only if the CSP is unable to provide the services without the use of the sub-processor objected to. This model could be of help especially where provisions are included in the contract defining criteria for the selection of new sub-processors and providing that such criteria must be met if the controller's failure to object within a given deadline is to be interpreted as an authorisation.<sup>40</sup>

### **2.3. Processing activities of the CSP for its business purposes**

- CSPs process some personal data in order to provide cloud services to PA and, in some cases, for their own business purposes. However, following the investigation activities, it appears that national stakeholders are not fully aware of the categories of personal data collected in this respect and the specific purposes for which they are processed - mainly because of the very high-level wording usually included in the CSP's model contracts.
- GDPR provision concerned: Articles 5, 6, 9 and 28 (28.3 and 28.10 in particular).
- In particular, for SaaS services, some CSPs' standard contracts envisage that the CSP could act as a data "controller" in relation to the processing of personal data in connection with its business operations. In these cases, it appears that the data protection regimes applicable to personal data collected and processed by CSPs for their own purposes may be other than those envisaged for the personal data processed on behalf of the PA (i.e., the CSPs usually apply the data protection rules they are subject to in respect of the personal data they process for providing the cloud services and for the business operations rather than the specific safeguards included in the Data Processing Agreements/Addendums signed with the PA).
- Upon specific requests, in some cases, CSPs provided the PA with additional information in this regard (e.g., in one case, it was explained that they considered all personal information collected or generated during the provision and administration of their cloud services as 'service data' they processed as a controller, including any "diagnostic data" related to how those services are used).

---

<sup>40</sup> EDPB, *Guidelines 07/2020*, paragraph 157, p. 43.

- Unclear information about the categories of personal data collected/generated from users of cloud services and the business purposes for which such data are processed raises concerns in relation to the appropriate legal basis for such kind of processing carried out by the CSPs as well as regarding compliance with the different obligations and responsibilities applying to controllers and processors in relation to the cloud services provided. From this perspective, a further assessment exercise should be carried out taking into account that, according to Article 28(3) GDPR, processors should process personal data only on documented instructions from the controller unless required to do so by Union or Member State law to which the processor is subject. This is all the more important for cases where ‘service data’ could be related to users other than the PA employees, i.e. to the individuals to whom public services are provided by the public authority (e.g., public Wi-Fi users, students using e-learning platforms, etc.).
- In this context, a few contractual changes have been negotiated in a specific case, on the PA’s request, aimed at limiting the processing of personal data by the CSP for its own purposes.
- This issue seems to have a more limited impact when cloud services are deployed as PaaS or IaaS considering that the amount of personal data ‘generated’ from the use of these services is far less substantial than the one ‘generated’ when SaaS are involved.

### **3. On International transfers and access by foreign public authorities**

#### **3.1. Transfer awareness and instructions on transfers**

- In relation to transfer awareness, the circumstance that the European region is specified in most cases as the place for the processing of personal data by CSPs would appear to give a wrong impression that no transfers are taking place. Only after the investigation activities and some specific questions related to provisions included in the Data Processing Agreements/Addendums referring to possible transfers, did some public authorities realize that data at rest is usually stored in the selected region, however there could be cases where the CSP cannot provide a service from the selected region as it needs to transfer data to third countries (e.g. typically in the case of ‘round the clock’ services); accordingly, the only way to avoid the transfers of personal data would be by refraining from use of the service at issue. Furthermore, this is usually the case with the processing of personal data for the CSPs’ own business purposes (see previous point).
- In some cases, a list of the services that cannot be provided without transferring personal data to third countries is provided to the PA; in other cases, the situation concerning transfers is less clear as they may depend on the possible use of individual services provided by sub-processors established in third countries, which are only referred to in bulk in the list of (possible) sub-processors (see previous point n. 4 on the difficulties in identifying the actual sub-processors involved in the processing of personal data on behalf of each relevant PA and consequences on the fulfilment of Article 30 GDPR – see point 9).
- GDPR provisions concerned: Article 5(1)a and 5(2), 28(3)a and Chapter V.
- In order to frame these possible transfers, it is usual for Data Processing Agreements/Addendums, as unilaterally drafted by the CSPs, to refer to SCCs as the tool to be used ‘in case’ of transfers. However, those SCCs are not accompanied by specific Annexes describing the specific (possible) transfers at issue. Annexes to the SCCs attached to the CSPs’ model contracts signed by the PA are always the same and do not contain any specific description of the (possible) flows of personal data in relation to the cloud services provided to the relevant PA; in fact, the wording in the Annexes is the same as the (general) one contained in the CSPs’ model contracts. For example, some annexes of SCCs for processor-to-processor transfers attached to the CSPs’ model contracts refer to the competence vested in the Supervisory Authority of the EEA processor, while it should

be clear that the competent Supervisory Authority to be referred to is the one competent for (each) relevant PA in case of processing activities carried out on behalf of PAs.

- While one could argue that that this model depends on the need to frame services provided worldwide by the CSPs to thousands of controllers, on the other hand, merely attaching the SCCs to the model contracts without any clear indication of the possible flows of data that they may cover risks undermining the controller's role and responsibilities in case of transfers pursuant to Article 28(3)a GDPR.
- Furthermore, mainly because of the lack of awareness about the possible existence of data transfers, generally, no transfer impact assessment is carried out by the PA and, even when it is carried out, it does not always cover all possible data transfers and third countries involved. In this respect, some stakeholders complained that it would be very difficult to assess the legislation of all third countries where possible processors may be established, especially where there is a lack of information about the sub-processors that are actually involved in the services provided to the PA. The lack of awareness on data transfers and the subsequent failure to assess the third countries involved in the possible transfers also impact the need to assess if the obligations set forth in the specific transfer tools can be complied with by the CSPs where the legislation of the third country may impinge on those obligations. After the Schrems II case, CSPs integrated their model contracts by Addendums referring to some additional measures in relation to the obligations to carry out an assessment of the legislation of the third country to which data are transferred and to adopt supplementary measures, where necessary, so as to ensure that the level of protection afforded by the GDPR would not be undermined once data are transferred. However, as clarified in the Recommendation 1/2020 on supplementary measures, there could be cases where the processor retains access to data in the clear following transfers or needs to access data in the clear in at least some cases, for example when scanning for security threats and, in those cases – similar to those described in use cases 6 and 7 of the EDPB Recommendations 01/2020 – it could be difficult to identify effective supplementary measures given the particular circumstances of the processing.

### **3.2. Access by government authorities of a third country to data within the EU/scope of the GDPR**

- Access requests issued by public authorities of third countries could also be addressed to CSPs established in the EU/EEA. In such cases, Article 48 GDPR should apply, providing for the safeguards necessary to ensure that the level of protection afforded by the GDPR would not be undermined. However, there could be an issue where the CSP receiving the request for access is part of a multinational group to which third country laws may apply. This may happen, in particular, taking into account the scope of certain foreign legislations, especially in the field of law enforcement or in the field of national security, which allow their public authorities to request access to data outside their own territory. Indeed, in these cases, requests can be addressed to companies which fall within the scope of these legislations. Therefore, in some situations, third countries' legislations deemed problematic in case of transfers would also apply within the EU/EEA and to data of EU/EEA data subjects without any initial transfer.
- GDPR provision involved: Articles 28 and 48.
- In this context, even where no data is transferred beforehand, the responsibility of PA could be engaged with regard to their CSPs on the basis of Article 28 which requires controllers to only use processors providing sufficient guarantees to implement appropriate technical and organisational

measures in such a manner that processing will meet the requirements of the Regulation and ensure the protection of the rights of the data subject.

- As a matter of fact, in their model contracts, almost all CSPs refer to the need to transfer personal data in order to ‘comply with law’. However, in no case is it clarified which ‘law’ is referred to, i.e. if this refers to EU MS laws or the laws of other countries (and, in some cases, general information is provided to the PA in relation to the way in which those requests are processed and some safeguards put in place).
- Clauses of this kind carry a huge risk for the PA as they are often included in the model contracts as authorised exceptions to the requirement of processing personal data in the EEA region; therefore, they result in instructions to process personal data in a way that may undermine the level of protection afforded by the GDPR as far as they allow processors to abide by third country laws which may impose restrictions on data protection rights that are not proportionate and necessary in a democratic society. In this respect, it would be essential for the PA to identify exactly the possible cases at stake in order to ensure that the requirements of the Regulation (including a valid legal basis and the respect of Chapter V provisions for any transfer to be carried out, the transparency obligations, the security measures) will be met and the protection of the rights of the data subject ensured.
- Where those processing activities (i.e., the disclosure of personal data by the processor in case of request by a third country public authority) are not referred to in the contracts, it should be borne in mind that Article 28(3)a GDPR allows for processors not to operate on the controller’s instructions only where required to do so by Union or Member State law (i.e., not by a third country law). Furthermore, Article 48 GDPR contains requirements that have to be met both by controllers and by processors and, as a matter of fact, are not referred to in the Data protection Agreements/addendums proposed by the CSPs.
- With regard to this issue, some mitigating factors identified by stakeholders for IaaS or PaaS services consist in adopting security measures such as encryption which may impede access to data in the clear if the decryption key is retained by the PA; however, such a mitigating factor cannot be adopted in case of SaaS services. Furthermore, there is a risk that no safeguards would be put in place if informing the controller on possible access requests by third country public authorities is prohibited beforehand (which could happen in most cases).

#### 4. **On telemetry data**

##### 4.1. **Difficulties in identifying the personal data at stake and understanding the processing activities carried out by the CSP, including international transfers**

- In order to provide the services, all CSPs collect and process telemetry data, i.e. data relating to the use of infrastructures and services (resource identifiers, tags, security and access roles, rules, usage policies, permissions, usage statistics) by different kind of users (e.g. employees, public Wi-Fi users, students, etc...). In particular, this data may be used e.g. to detect, identify and respond to operational issues, such as identifying and patching bugs and fixing problems, or to measure, support, and improve the services provided. Technical and organizational measures to protect personal data processed are generally adopted by the CSPs; data may be anonymized (e.g. by default avoiding the collection of personal data) or pseudonymized and rules are usually set forth in order to minimize human access to usage and diagnostic data and avoid the identification of individuals. However, from a data protection point of view, the exact role of the CSPs when processing this kind of data should be clarified. In some cases, they declare they act as controllers while in others they consider themselves as processors on behalf of the PA.

- GDPR provisions involved: Articles 5, 6, 28.
- In most cases, stakeholders do not appear to pay special attention to these processing activities and additional information was sought from the CSPs only because of the investigation activities. In some cases, the information provided was not precise enough and additional information was requested. However, considering the huge amount of personal data that may be collected, a more careful assessment on the part of the PA would be essential, in particular where telemetry data may be collected with regard to the end-user of the services (e.g. individuals to whom a service is provided by the PA). Clarifying the exact role played by the CSPs when processing telemetry data is essential in order to identify the appropriate legal basis and ensure the respect of Article 5 GDPR principles with particular regard to transparency, purpose limitation and data minimisation.

## **5. On Compliance**

### **5.1. Audit**

- As a preliminary result of the enforcement action, it seems to be a common approach for all involved stakeholders to carry out periodic checks on CSPs' activities through the annual verification of the certification reports and the documentation made available by the CSP on the website; by analysing the security reports of independent bodies; or via checklists prepared by the PA to assess the compliance by the CSP with the contractual clauses and current legislation on the processing of personal data. Thus, it appears that, so far, no public authority has carried out specific and direct audit activities, including inspections, regarding any CSPs.
- GDPR provision involved: Article 5(2) and 28(3)(h).
- Some stakeholders complained that generally the CSPs do not allow the performance of audits by customers and that it is difficult to negotiate specific clauses in this regard (such as obtaining access to the results of audits carried out by third parties or requesting that third parties focus their audit on specific aspects indicated by the PA).

### **5.2. Record of processing activities of the CSP in relation to the specific controller/public administration**

- As a preliminary result of the enforcement action, it appears that CSPs do not hold a specific record of processing activities carried out on behalf of each PA. When a record of the processing activities is in place, it is of a general nature and refers to all the activities carried out by the processor in relation to the services provided to all customers/controllers.
- GDPR provision involved: Article 30(2).
- Upon specific requests, some CSPs did not reply, others referred to their own websites for information on the processing activities carried out, others sent a very general record which did not contain all of the elements set forth by Article 30(2) (a-d) GDPR,
- In one case, it was also considered that it was not possible for the CSP to hold a record of the specific processing activities for each customer, since the CSP had no information on the types/categories of the processed data, nor of the purposes of the processing and the services actually used by customers (it was explicitly considered that the CSPs do not restrict the publicly available services the customer may choose to use).

### Part III – Actions by the SA

1. Have you taken action (i.e. fact-finding exercises, informal contact, prior consultation, investigation) towards any of the stakeholders concerning the use of cloud-based services prior to launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).
  - Prior to launching the coordinated action, the IT SA has adopted the following decisions in the field of cloud computing:
  - On 23 November 2021<sup>41</sup>, the IT SA issued a favorable opinion, with some comments, on a draft Decree of the Ministry of Foreign Affairs on the testing of electronic voting in elections for the renewal of Committees of Italians Abroad. In issuing the opinion, the Authority requested clarifications in the decree about the role carried out by the Ministry and other parties involved (e.g. Cloud service provider) and highlighted the need to envisage the data retention period of data. Besides, the Ministry was also required to take additional measures in case of transfer of personal data in third countries to ensure a level of protection of personal data substantially equivalent to that provided for in the EU, including the encryption of personal data by the controller, with encryption keys in its exclusive availability.
  - On 16 September 2021<sup>42</sup>, in a decision on a complaint relating to the ‘proctoring system’ called Respondus used by an Italian University, the IT SA declared the unlawfulness of the processing carried out by the University on account of the infringement of Articles 5 (1) (a), (c) and (e), 6, 9, 13, 25, 35, 44 and 46 of the GDPR and Section 2-f of the Italian Data Protection Code and prohibited the University from further processing students’ biometric data and data on the basis of which the profiling of data subjects through the Respondus system is carried out. The Authority prohibited also the transfer of data subjects’ personal data to the United States of America in the absence of adequate safeguards for such data subjects as a result of the absence of an appropriate and documented assessment of the relevant third country law in the light of the Schrems II ruling and issued a fine of EUR 200.000,00 (two hundred thousand).
  - In June 2021<sup>43</sup>, as a result of an on own volition enquiry, the IT SA found infringements of the GDPR arising from the configuration of the ‘IO’ app, a public administration app used as access point to local and national public services in Italy (among others, for example, related to payments towards PAs, EU Digital COVID certificates, communication from PAs to citizen, etc.), in relation to excessive data collection and transfer to third countries, inadequate information to users, failure to request users’ consent for storing information, or accessing information that is already stored, in their terminal equipment, unnecessary geolocation of users based on IP addresses. The Garante ordered to provisionally limit certain data processing activities as performed via the said app since they entailed interactions with services by Google and Mixpanel and resulted accordingly into transfers to third countries of data that are highly sensitive including information on cashback transactions and payment tools. After the publicly-owned company managing the App committed themselves to minimize user data collected for the purpose of activating the

<sup>41</sup> <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9721434>

<sup>42</sup> <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9703988>. The decision is currently under judicial proceeding.

<sup>43</sup> <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9668051> and <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9670061>

services provided through the ‘IO’ app and transferred to third countries and to implement the corrective measures requested by the SA (e.g. several functions were deactivated as they allowed tracing user location via his or her IP address and unnecessary Google services were deactivated and steps were taken to prevent the contents of push notifications from being disclosed to Google and Apple), the Italian SA lifted the temporary limitation it had imposed on the processing of personal data. However, the processing will continue to be limited as for the data collected and stored by Mixpanel. Those data may not be used any longer and will only be stored by the company until the SA completes its investigations (which are still ongoing).

- In January 2020<sup>44</sup>, the IT SA issued an opinion on the draft “Guidelines — Security in ICT procurement” setting out general guidelines for public administrations when dealing with IT acquisitions as well as public service providers. Among several recommendations, the Garante highlighted the need to adequately identify, as part of the tender specifications, a correct distribution of the respective responsibilities between the controller and processors, in particular avoiding disproportionate clauses relating to liability, especially in the case of standard contracts, with almost zero trading margins on the part of the data controller.
- 2. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (E.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**
- The investigations are still pending.

#### **Part IV – Other**

1. **What is your general impression of the levels of awareness and compliance of the stakeholders you consulted concerning the use of cloud?**
  - It seems that there is generally a lack of awareness about: 1. data transfers that can take place even despite the PA has identified the EEA as the selected region for the main processing activities; 2. the telemetry data processed by the CSPs; 3. Request for access to personal data stored in the EEA by third country public authorities.
2. **Are there any other issues or topics that you would like to flag?**
  - None.
3. **Are there any leading practices of the stakeholders you have contacted that you would like to share?**
  - None for the time being.

---

<sup>44</sup> <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9283857>

**Part I – Statistics**

**4. How many stakeholders have you contacted within the following categories?**

- Ministry of the central government
- Independent public body of the central government
- Buyer for the central government (1)
- Publicly-owned company acting as a processor for several central public bodies
- Ministry of the regional government
- Independent public body of the regional government
- Buyer for the regional government
- Publicly-owned company acting as a processor for several regional public bodies
- Other, please specify

**5. How many stakeholders have you contacted within the following sectors?**

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government
- Economic affairs
- Education
- Finance
- Health
- Infrastructure
- Employment
- Justice
- Tax
- Other, please specify: **We did not contact a stakeholder from a specific sector, but the IT department as the buyer for the central government.**

**6. If you have contacted a buyer, for which sectors does this buyer provides its services:**

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government
- Economic affairs
- Education
- Finance
- Health
- Infrastructure
- Employment
- Justice
- Tax
- **No specific sector**
- Other, please specify

**7. If you have contacted a buyer, and if you have this information, please specify the number of stakeholders this buyer provides services for:**

- 39 departments

**8. What was the initial procedural framework of your action?**

- **Fact finding**
- Fact finding + determining follow-up action based on the results
- New investigation<sup>45</sup>
- Ongoing investigation

**9. How many stakeholders indicated that they use CSPs or are planning to do so in the near future (end of 2022)?**

- The central buyer gave us 5 examples of CSPs that are used or planned to be used in the near future.

**10. Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?**

- Internal organisation (office suites, internal communication, HR, etc.): **All 5 CSPs examined**
- Exercise of public functions (services to citizens, processing citizen's data, etc.)

**11. For the following commonly identified sectors, please specify if any hyper-scalers<sup>46</sup> are involved (if so please name them) either because they provide the services themselves or because the services are using the infrastructures of these hyper-scalers**

- Health
- Finance
- Tax
- Education
- Central buyers or providers of IT services: **Cloud services of Microsoft and AWS are (planned to be) used.**

**12. How many stakeholders took the following actions prior to- or during the acquisition of a CSP?**

- Perform a DPIA: **Only for one CSP, a DPIA was performed.**
- Does the DPIA analyse transfers in details (sometimes called DTIA): **No, however, for a second CSP a risk-based analysis of transfers was performed (Rosenthal).**
- Contact the DPO for advice: **Yes.**
- Perform a general risk analysis: **A general risk analysis is being performed for every CSP procured.**
- Contact the SA for advice: **The SA was contacted regarding 1 CSP that is planned to be used.**

**13. How many stakeholders (including buyers) take the following actions during the use of the CSP?**

- Monitoring technical and organisational measures to ensure compliance: **When procuring the CSP, monitoring of technical and organisational measures to ensure compliance is performed. After that, monitoring is only performed in a non-systematic way (ad hoc), e.g. when a technical issue comes up, a legal decision becomes known, a new version of an application is rolled out, new categories of data are processed, etc.**
- In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g. Schrems II): **When procuring the CSP, technical and organisational measures such as encryption (data in transit, data at rest and key management), server location, identity access**

---

<sup>45</sup> making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred

<sup>46</sup> Hyper-scalers provide cloud services at scale. It refers usually to the big cloud providers (Google, AWS, Microsoft ...) on which other services may also depend

- management, Cloud Access Security Broker (CASB) services are planned or have already been implemented. After that, adoption of technical and organisational measures and monitoring are only performed in a non-systematic way (see above).
- Regular risk assessments: When procuring the CSP, a risk assessment is performed. After that, risk assessment is only performed in a non-systematic way, not on a regular base (see above).

## Part II – Substantive issues

### 1. Pre-contractual phase: Determining sufficient guarantees with regards to appropriate technical and organisational measures

#### 1.1. Brief description:

- The central buyer tries to implement appropriate technical and organisational measures to ensure compliance of the CSP selected with GDPR. In particular, the central buyer tries to make sure that the location of the server is in Europe and that adequate encryption technologies are applied (data in transit/ data at rest). In addition, identity access management (IAM) and Cloud Access Security Broker (CASB) services are planned or have already been implemented. Whether these measures can be seen as sufficient in the context of international data transfers has to be further investigated. In addition, some contracts seem to allow the CSPs (and/or their sub-processors) to process large amounts of personal data other than the user data, e.g. telemetry data, for their own purposes and at locations elsewhere than where the server of the user data is located. It still has to be clarified, whether there are sufficient guarantees with regards to appropriate technical and organisational measures in all of the contracts and/or in the buying-process, ensuring protection of all personal data processed.

#### 1.2. Provision(s) of the GDPR (or national laws) concerned:

- A processing of personal data for own purposes of the CSP without a legal base would infringe Art. 5 (1) a and Art. 6 (1) GDPR.
- A transfer of such data to third countries without any/sufficient guarantees according to chapter V GDPR would infringe Art. 44 GDPR.
- A lack of appropriate technical and organisational measures would infringe Art. 24 (1) and (2), Art. 25 as well as Art. 32 GDPR.
- A lack of sufficient guarantees thereof in the contract would infringe Art. 28 GDPR.

#### 1.3. Why this has been an issue:

- It has to be clarified, how the central buyer can be supported in the pre-contractual phase, to avoid potential issues when determining sufficient guarantees with regards to appropriate technical and organisational measures.

#### 1.4. (Potential) solution(s):

- Central buyer: If it were established, that in any of the contracts with CSPs there are not sufficient guarantees with regards to appropriate technical and organisational measures, these contracts would have to be renegotiated to ensure compliance with GDPR of all data processing involved. In cases where this were not possible, the use of the CSP (or projects to use a certain CSP) would have to be terminated.
- Central buyer: Additional support in analysing and understanding contracts offered by CSPs and legal frameworks involved could be provided by a legal officer specifically in charge of this task. The legal officer could then also help negotiating GDPR-compliant contracts and implementing sufficient guarantees with regards to appropriate technical and organisational measures.

- Central buyer: The DPO should play an active role in the analysis and negotiation of contracts offered by CSPs as well.
- SA: The SA will continue to raise awareness regarding the issues and risks associated with the use of CSPs and stands ready to give advice to the central buyer.

## **2. Contract with CSP: Risk mitigating measures within the contract**

### **2.1. Brief description:**

- The central buyer tries to implement risk-mitigating measures within the contracts with CSPs. In particular, the central buyer tries to make sure that the location of the server is in Europe and that adequate encryption technologies are applied (data in transfer/ data at rest). However, especially with regards to US-based CSPs, the central buyer repeatedly finds itself in the situation that it either has to accept the terms offered in the contract by the CSP or has to withdraw, as there is no possibility to negotiate additional risk mitigating measures with the CSP. Furthermore, some of the contracts with the CSPs seem to allow the CSPs (and/or their sub-processors) to process large amounts of personal data other than the user data, e.g. telemetry data, for their own purposes and at locations elsewhere than where the server of the user data is located. It has to be clarified yet, whether there are enough risk mitigating measures incorporated within all of the contracts, ensuring adequate protection of data.

### **2.2. Provision(s) of the GDPR (or national laws) concerned:**

- A processing of personal data for own purposes of the CSP without a legal base would infringe Art. 5 (1) a and Art. 6 (1) GDPR.
- A transfer of such data to third countries without any/sufficient guarantees according to chapter V GDPR would infringe Art. 44 GDPR.
- A lack of (sufficient) risk mitigating measures would infringe Art. 24 (1) and (2), Art. 25 as well as Art. 32 GDPR.
- A lack of them within the contract with a CSP would also infringe Art. 28 GDPR.

### **2.3. Why this has been an issue:**

- The central buyer of the Principality of Liechtenstein is a rather small customer of CSP services. Because of this, it does not have sufficient negotiating power when it comes to terms and conditions offered in contracts of big CSPs. Therefore, the central buyer repeatedly finds itself in the situation that it can either accept contracts that do not contain sufficient risk mitigating factors or has to withdraw. It has to be clarified, how the central buyer can be supported in negotiating adequate risk mitigating measures with a CSP.

### **2.4. (Potential) solution(s):**

- Central buyer: If it were established, that any of the contracts with CSPs do not contain sufficient risk mitigating measures, these contracts with CSPs would have to be renegotiated to ensure compliance with GDPR of all data processing involved. In cases where this was not possible, the use of the CSP (or projects to use a certain CSP) would have to be terminated.
- Central buyer: Additional support in analysing and understanding contracts offered by CSPs and legal frameworks involved could be provided by a legal officer specifically in charge of this task. The legal officer could then also help negotiating adequate risk mitigating measures within the contract with a CSP.
- Central buyer: The DPO should play an active role in the analysis and negotiation of contracts offered by CSPs as well.
- SA: The SA will continue to raise awareness regarding the issues and risks associated with the use of CSPs and stands ready to give advice to the central buyer.

### **3. Contract with CSP: Negotiating a bespoke contract**

#### **3.1. Brief description:**

- The central buyer tries to negotiate bespoke contracts with CSPs. It has done so successfully, e.g. when negotiating that the location of the server is in Europe and that adequate encryption technologies are applied (data in transfer/ data at rest). On other occasions, however, especially with US-based CSPs, the central buyer apparently found itself in the situation that it could either accept the terms and conditions offered in the contract by the CSP or had to withdraw, as there was no possibility to negotiate additions or amendments to it. As a result, some contracts were not closed at all and others are not fully tailor-made to the needs of the central buyer, but reflect (in parts) the non-negotiable clauses offered by the CSP (and/or its sub-processors). It has to be further investigated yet, whether these pre-specified clauses ensure adequate protection of data.

#### **3.2. Provision(s) of the GDPR (or national laws) concerned:**

- A processing of personal data for own purposes of the CSP without a legal base would infringe Art. 5 (1) a and Art. 6 (1) GDPR.
- A transfer of such data to third countries without any/sufficient guarantees according to chapter V GDPR would infringe Art. 44 GDPR.
- A contract with a CSP not covering all the data protection requirements according to GDPR would infringe Art. 28 GDPR.

#### **3.3. Why this has been an issue:**

- The central buyer of the Principality of Liechtenstein is a rather small customer of CSP services. Because of this, it does not have sufficient negotiating power when it comes to terms and conditions offered in contracts of big CSPs. Therefore, it repeatedly found itself in the situation that it could either accept (parts of) pre-specified contracts or had to withdraw. It has to be clarified, how the central buyer can be supported in negotiating bespoke contracts with CSPs.

#### **3.4. (Potential) solution(s):**

- Central buyer: If it were established, that any of the contracts / clauses in contracts with CSPs do not fully respond to the requirements of the central buyer, these contracts / clauses in contracts with CSPs would have to be renegotiated to ensure GDPR-compliance for all data processing involved. In cases where this were not possible, the use of the CSP (or projects to use a certain CSP) would have to be terminated.
- Central buyer: Additional support in analysing and understanding contracts offered by CSPs and legal frameworks involved could be provided by a legal officer specifically in charge of this task. The legal officer could then help negotiating bespoke clauses within the contract with a CSP.
- Central buyer: The DPO should play an active role in the analysis and negotiation of contracts offered by CSPs as well.
- SA: The SA will continue to raise awareness regarding the issues and risks associated with the use of CSPs and stands ready to give advice to the central buyer.

### **4. International transfers and access by foreign public authorities: transfer awareness**

#### **4.1. Brief description:**

- The central buyer tries to handle international data transfers and the potential access by foreign public authorities according to the requirements of GDPR. He does that primarily by choosing European CSPs or in establishing that at least the location of the server is in Europe and that adequate encryption technologies are applied (data in transfer/ data at rest). Beyond that, the central buyer tends to apply a risk-based approach to evaluate the sensitivity of the data processed by the CSP and the legal framework of the country of the CSP. Besides, the answers to the questionnaire seem to indicate that the central buyer might not be fully aware that some

European CSPs use sub-processors (especially US-based CSPs) that are processing personal data for own purposes as well and/or transfer them to third countries. Furthermore, some contracts with the CSPs also allow the CSPs (and/or their sub-processors) to process large amounts of personal data other than the user data, e.g. telemetry data, for their own purposes and at locations elsewhere than the server of the user data. As a result, it has to be investigated whether there are sufficient safeguards according to chapter V GDPR in all of the contracts for the adequate protection of data. It seems to be the case therefore, that transfers of personal data to third countries are taking place in some of the contracts and potential access by foreign public authorities to the data cannot be excluded. This is subject to further investigation, however.

#### **4.2. Provision(s) of the GDPR (or national laws) concerned:**

- A transfer of personal data to third countries without any/sufficient guarantees according to chapter V GDPR would infringe Art. 44 ff. GDPR.
- A transfer /disclosure of personal data to foreign public authorities might also infringe Art. 48 GDPR.
- A potential access to personal data by foreign public authorities might – under certain circumstances – infringe Art. 5 (1) f GDPR.
- A selection of a processor/sub-processor who cannot adhere to the principles of GDPR would infringe Art. 28 (1) and (3) a GDPR.

#### **4.3. Why this has been an issue:**

- Every time the central buyer did not find an equivalent European CSP to a third country-CSP, it tried to mitigate the risks of the data processing / transfers and of potential access by foreign public authorities as far as possible (e.g. server location in Europe, encryption of data, IAM and CASB solutions, processing of non-sensitive data only, etc.). However, according to the answers to the questionnaire, the central buyer seems to only have assessed the actual CSP and its data processing, but not all the sub-processors used by a CSP as well. Neither does the central buyer seem to have assessed the potentially abundant data processing for own purposes of some CSPs (and/or their sub-processors) and in third countries (e.g. telemetry data), which also could involve international data transfers.
- In order to establish, whether these presumed shortcomings come true and whether the risk mitigating measures taken by the central buyer are sufficient to ensure adequate protection of the (transferred) personal data, a further in-depth investigation will be required. Furthermore, it has to be clarified, how the central buyer can be supported in raising its awareness of international data transfers and of (potential) access by foreign public authorities as well as of the risks/issues associated with it.

#### **4.4. (Potential) solution(s):**

- Central buyer: If it were established, that any of the contracts with CSPs comprise international data transfers that do not comply with chapter V GDPR, these contracts with CSPs would have to be renegotiated to ensure compliance with GDPR of all data processing involved. In cases where this were not possible, the use of the CSP (or projects to use a certain CSP) would have to be terminated.
- Central buyer: Additional support in analysing and understanding contracts offered by CSPs and legal frameworks involved could be provided by a legal officer specifically in charge of this task. The legal officer could then also help negotiating GDPR-compliant contracts covering all data processing foreseen in them.
- Central buyer: The DPO should play an active role in the analysis and negotiation of contracts offered by CSPs as well.

- SA: The SA will continue to raise awareness regarding the issues and risks associated with the use of CSPs and stands ready to give advice to the central buyer.

## 5. **Telemetry data**

### 5.1. **Brief description:**

- The central buyer sincerely tries to negotiate GDPR-compliant contracts with CSPs. He does that primarily by establishing that the location of the server is in Europe and that adequate encryption technologies are applied (data in transfer/ data at rest). In addition, identity access management (IAM) and Cloud Access Security Broker (CASB) services are planned or have already been implemented. However, some contracts with the CSPs seem to allow that the CSPs (and/or their sub-processors) process large amounts of personal data other than the user data, e.g. telemetry data, for their own purposes and at locations elsewhere than the server of the user data. As a result, it has to be further investigated whether there are enough guarantees found in some of the contracts, ensuring adequate protection of those data as well.

### 5.2. **Provision(s) of the GDPR (or national laws) concerned:**

- A processing of personal data, such as telemetry data, for own purposes of the CSP without a legal base would infringe Art. 5 (1) a, b, c and Art. 6 (1) GDPR.
- A transfer of such data to third countries without any/sufficient guarantees according to chapter V GDPR would infringe Art. 44 GDPR.
- A lack of adequate data protection clauses covering also telemetry data in the contract with a CSP would infringe Art. 28 GDPR.

### 5.3. **Why this has been an issue:**

- It has to be clarified, how the central buyer can be supported to avoid potential issues regarding the processing of telemetry data by CSPs (and/or their sub-processors).

### 5.4. **(Potential) solution(s):**

- Central buyer: If it were established, that any of the contracts with CSPs comprise an unlawful processing of telemetry data by the CSP (and/or its sub-processors), these contracts with CSPs would have to be renegotiated to ensure GDPR-compliance for all data processing involved, including processing of telemetry data. In cases where this were not possible, the use of the CSP (or projects to use a certain CSP) would have to be terminated.
- Central buyer: Additional support in analysing and understanding contracts offered by CSPs and legal frameworks involved could be provided by a legal officer specifically in charge of this task. The legal officer could then also help negotiating GDPR-compliant clauses concerning the processing of telemetry data by the CSP.
- Central buyer: The DPO should play an active role in the analysis and negotiation of contracts offered by CSPs as well.
- SA: The SA will continue to raise awareness regarding the issues and risks associated with the use of CSPs and stands ready to give advice to the central buyer.

## Part III – Actions by the SA

1. **Have you taken action (i.e. fact-finding exercises, informal contact, prior consultation, investigation) towards any of the stakeholders concerning the use of cloud-based services prior to launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the stakeholder, general guidance,**

**corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

- We have roughly outlined the data protection related risks and issues connected to the use of MS 365 in the framework of a general risk analysis performed by the central buyer.
- 2. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (E.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing).**
  - We plan to inform the central buyer of the results of the CEF and thus of the general direction of dealing with CSPs in the EEA as defined by the EDPB. This should raise awareness, but also provide legal guidance and negotiating power for the central buyer when assessing / procuring CSPs.

#### **Part IV – Other**

1. **What is your general impression of the levels of awareness and compliance of the stakeholders you consulted concerning the use of cloud?**
  - Compliance is very good in several areas, but in other areas there seem to be some gaps and further investigation has to be performed. Besides, as there is no established European best practice regarding CSPs like MS 365 etc. yet, the central buyer tends to apply mainly a risk-based approach with regards to international data transfers.
2. **Are there any other issues or topics that you would like to flag?**
  - No
3. **Are there any leading practices of the stakeholders you have contacted that you would like to share?**
  - No

# LT SA

State Data Protection Inspectorate (hereinafter – Lithuanian SA)

## Part I – Statistics

1. **How many stakeholders have you contacted within the following categories?**

- 1. Independent public body of the central government

2. **How many stakeholders have you contacted within the following sectors?**

- Other, please specify: 1. Statistics Lithuania (hereinafter – stakeholder)

3. **If you have contacted a buyer, for which sectors does this buyer provides its services:**

- N/A

4. **If you have contacted a buyer, and if you have this information, please specify the number of stakeholders this buyer provides services for:**

- N/A

5. **What was the initial procedural framework of your action?**

- Fact finding + determining follow-up action based on the results
- Ongoing investigation

6. **How many stakeholders indicated that they use CSPs or are planning to do so in the near future (end of 2022)?**

- 1

7. **Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?**

- Internal organisation (office suites, internal communication, HR, etc.) : 1
- Exercise of public functions (services to citizens, processing citizen's data, etc.): 1

8. **For the following commonly identified sectors, please specify if any hyper-scalers<sup>47</sup> are involved (if so please name them) either because they provide the services themselves or because the services are using the infrastructures of these hyper-scalers:**

- Health
  - Finance
  - Tax
  - Education
  - Central buyers or providers of IT services
- 
- CSP Palantir uses Amazon Web Services, Inc. (AWS) and Microsoft Corporation. AWS provides the cloud infrastructure for Palantir products. Microsoft Corporation uses for provision of cloud infrastructure to host Active Directory for CentralAuth.
  - CSP Microsoft provides the services themselves.

9. **How many stakeholders took the following actions prior to- or during the acquisition of a CSP?**

---

<sup>47</sup> Hyper-scalers provide cloud services at scale. It refers usually to the big cloud providers (Google, AWS, Microsoft ...) on which other services may also depend

- Perform a DPIA: **none**
- Does the DPIA analyse transfers in details (sometimes called DTIA): **none**
- Contact the DPO for advice: **none**
- Perform a general risk analysis: **none**
- Contact the SA for advice: **none**

**10. How many stakeholders (including buyers) take the following actions during the use of the CSP?**

- Monitoring technical and organisational measures to ensure compliance: **none**
- In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g. Schrems II): **none**
- Regular risk assessments: **none**

## Part II – Substantive issues

**1. Data protection impact assessment (Article 35 GDPR).**

**1.1. Name the issue and briefly describe the main issue(s) identified.**

- The audited stakeholder uses the services of three CSPs for data processing:
  - The stakeholder has concluded Palantir Foundry (a cloud-based database management platform) licensing agreement with CSP Palantir Technologies UK, Ltd., including platform support, along with infrastructure services.
  - Services provided by Microsoft Corporation include Office program data synchronization / transfer services – e-mail and group work data exchange service, website and workspace hosting service, communication service, user data cache (products as Office 365, OneDrive, Teams).
  - Services provided by CSP Information Society Development Committee (CSP ISDC) (public institution under the Ministry of Economy and Innovation of the Republic of Lithuania) are used for internal administration and public functions (contracts, information systems administration, statistical surveys, human resources management).
- In none of the three cases data protection impact assessment (DPIA) has been carried out.

**1.2. Which provision(s) of the GDPR (or national laws) does this concern?**

- According to GDPR Article 35 (3) (b) a DPIA referred to in paragraph 1 shall in particular be required in the case of processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10. In the information systems, the data of which is processed on the cloud-based platforms, personal data is processed on a large scale, and cloud services are used for processing personal data, which can be evaluated as an innovative technology for data processing. It should be noted that the information systems process on a large-scale personal data of extremely vulnerable data subjects and special personal data categories such as special categories of data referred to in GDPR Article 9(1) (for example, health data) and personal data relating to criminal convictions and offences referred to in GDPR Article 10. The exceptions specified in Articles GDPR Article 35 do not apply, therefore Lithuanian Department of Statistics had the obligation to perform DPIA in all three cases before starting to use services based on cloud technology for processing personal data.

### **1.3. Explain why this has been an issue for your stakeholders?**

- Stakeholder takes the position that the technical and organizational measures applied by CSPs are sufficient and an assessment of the impact on data protection was not required, and this stakeholder also expressed the opinion that DPIA is not required when standard contractual conditions are applied.

### **1.4. What are differences that you have encountered between stakeholders in your Member State?**

- N/A. Lithuanian SA inspected only one stakeholder.

### **1.5. What are solutions to this issue? Please describe if these solutions are already implemented or potential, and whether this solution is provided by the SA or the stakeholders.**

- Lithuanian SA proposes to establish an obligation to carry out DPIA (GDPR Article 35(1)) and, if necessary, its review (GDPR Article 35(11)).

## **2. Problems with choosing specific CSPs and no contract negotiations.**

### **2.1. Name the issue and briefly describe the main issue(s) identified.**

- **Issue (1)** - CSP Palantir and CSP Microsoft terms of the contracts for cloud services were negotiated, they were accepted on a take-it-or-leave-it basis:
  - Pursuant to Palantir's declaration of exclusivity, in which Palantir together with all of its group companies and affiliates, affirms that it is the sole supplier of Palantir software (including Palantir Foundry) to the government and has an exclusive license to sell, install, support and update such software, Lithuanian SA found that the stakeholder did not select or evaluate any other cloud service providers. I.e., The State Data Management information system has been created on the basis of the Data management and analytics platform – Palantir Foundry, so the stakeholder has no other CSP option for this information system.
  - A Microsoft licensing agreement has been concluded with private company (not Microsoft). Since Microsoft license can only be purchased based on a standard contract, negotiations were not carried out. 2010 SCCs of Microsoft Corporation apply, Stakeholder has no direct written data processing agreement with Microsoft.
  - This indicates that the Stakeholder could not negotiate with the CSP on the terms of the contract in order to properly adjust the terms of the contract that they meet Stakeholder's requirements, and in the contracts, there are indicated possibilities to object on subproviders, but there are no provisions on the consequences of this objection (GDPR Article 28(2)). It is not clear whether the objection can be expressed without breaching the contract.
- **Issue (2)** – Sub-processors. Stakeholder has informed Lithuanian SA that it does not have any information/evidence that CSPs Palantir and CSP ISDC are actually using services of sub-processors based on contracts or other legal act in compliance with the provisions of the GDPR Article 28(4).

### **2.2. Explain why this has been an issue for your stakeholders?**

- **Issue (1)** – On the date of stakeholder signing Microsoft licencing agreement where 2010 SCCs apply, 2021 SCCs have already been approved by the EC, therefore stakeholder cannot be sure that data processing by Microsoft is sufficiently safe.

Stakeholder holds the position that they were in a position where they had to accept contracts on a take-it-or-leave-it basis without having power to negotiate.

- **Issue (2)** - Stakeholder may not have requested detailed and clear information /did not contact directly the CSPs Palantir and CSP ISDC about the verification of compliance with the GDPR Article 28(4).

#### **2.3. Which provision(s) of the GDPR (or national laws) does this concern?**

- **Issue (1)** - GDPR Article 28(2): The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall 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.

GDPR Article 28(3) states that Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

GDPR Article 28(9): The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

- **Issue (2)** -According to GDPR Article 28(4), CSP must provide sufficient guarantees that sub-processors implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation and Stakeholder.

#### **2.4. What are solutions to this issue? Please describe if these solutions are already implemented or potential, and whether this solution is provided by the SA or the stakeholders.**

- **Issue (1)** - Stakeholder should evaluate if CSP SCCs meet the requirements of GDPR and Stakeholder's requirements. Stakeholder must ensure compliance with the provisions of GDPR Article 28.
- **Issue (2)** – Stakeholder should be guaranteed that CSP's sub-processors implements appropriate technical and organisational measures in such a manner that the processing will meet the requirements of GDPR and Stakeholder's requirements.

### **3. International transfers and access by foreign public authorities.**

#### **3.1. Name the issue and briefly describe the main issue(s) identified.**

- Lithuanian SA was provided with only minimal information on the transfer of personal data to third countries and only on transfers to the US in the case of using CSP Palantir services. Stakeholder could not explain what personal data is transferred to the third countries, what technical and organizational measures are applied for such transfers.
- Stakeholder did not provide any information whether in the case of CSP Microsoft and CSP ISDC provided cloud services personal data is transferred to third countries.

#### **3.2. Explain why this has been an issue for your stakeholders?**

- Stakeholder indicated that standard data protection conditions are used for the transfer of personal data to third countries, but the EU SCCs that provide specific guarantees around transfers of personal data for in-scope services were not signed with CSP Palantir. Therefore, Lithuanian SA considers that failure to sign SCCs (2021) with Palantir does not obligate unconditional compliance with them and decent level of security.
- Stakeholder may not have requested detailed and clear information /did not contact directly the CSPs Microsoft and CSP ISDC on a matter of personal data transfers to the third countries.

**3.3. Which provision(s) of the GDPR (or national laws) does this concern?**

- GDPR Article 46(1): In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

**3.4. What are solutions to this issue? Please describe if these solutions are already implemented or potential, and whether this solution is provided by the SA or the stakeholders.**

- Lithuanian SA proposes to sign EU SCCs (2021) for the transfers of personal data to the third countries with the CSP Palantir in order to provide specific guarantees around transfers of personal data for cloud-based services.
- Verifying whether personal data is actually transferred to third parties using cloud services of CSP Microsoft and CSP ISDC. In the case of transfers implement the adequate measures in order to ensure compliance with the provisions of GDPR Chapter V.

**4. Collection and processing by the CSP of diagnostic/telemetry data (Article 5 GDPR).**

**4.1. Name the issue and briefly describe the main issue(s) identified.**

- *CSP Palantir collects and processes diagnostic / telemetric data (metrics, analysis, statistics, or other data) related to the stakeholder's use of the software (in case this data is anonymized).*
- *CSP Microsoft collects and manages diagnostic / telemetric data (providing users with unique IDs).*
- Stakeholder did not provide / specify the categories of personal data collected regarding the telemetric/diagnostic data processed by the *CSP Palantir* to Lithuanian SA.
- Stakeholder did not conduct an assessment of the data (including diagnostic / telemetric data) used by *CSP Palantir* and *CSP Microsoft* for their own purposes, nor did it specify where the anonymization is performed (on the client or on the *CSP* servers).

**4.2. Which provision(s) of the GDPR (or national laws) does this concern?**

- The principles of Article 5 of the GDPR that personal data must be processed in a lawful, fair and transparent manner in relation to the data subject (principle of lawfulness, fairness and transparency), collected for specified, clearly defined and legitimate purposes and not further processed in a manner incompatible with those purposes are not guaranteed, implemented. adequate, appropriate and limited to what is necessary to achieve the purposes for which they are processed (principle of data minimisation).

**4.3. Explain why this has been an issue for your stakeholders?**

- Because stakeholder may not have requested detailed and clear information /did not contact directly the CSP about the diagnostic / telemetric data being collected and processed. They were not analysed, nor were there any evaluations carried out before the start of usage, and in the contract did not provide clearly and precisely what could be collected.

**4.4. What are differences that you have encountered between stakeholders in your Member State?**

- N/A.

**4.5. What are solutions to this issue? Please describe if these solutions are already implemented or potential, and whether this solution is provided by the SA or the stakeholders.**

- A possible solution is to clearly provide in the CSP Palantir contract what diagnostic / telemetric data can be processed and when. Conduct a thorough assessment of them, requiring evidence from the CSP Palantir and CSP Microsoft. This decision is provided for by the Inspectorate, but has not yet been submitted to the stakeholder, and therefore has not been implemented.

**5. Monitoring of the implemented technical and organisational measures including security measures of the CSPs (Article 32 GDPR).**

**5.1. Name the issue and briefly describe the main issue(s) identified.**

- Stakeholder has not provided / submitted to Lithuanian SA any data safety risk assessment related to the stakeholder, which led to the fact that CSP Palantir, CSP Microsoft is the right solution for the stakeholder.
- Stakeholder did not provide any evidence to evaluate the CSP Palantir and CSP Microsoft, and the stakeholder did not provide any information to familiarize itself with the certification reports or summaries of the report of the CSP Palantir and CSP Microsoft.
- The stakeholder did not provide information / evidence that the CSP Palantir provides adequate organizational and technical security measures. The stakeholder did not provide a document or other evidence of what exactly technical and organizational measures are implemented. The stakeholder did not provide information / evidence regarding the technical and organizational security measures implemented by CSP Palantir, or after conducting a risk assessment.
- Stakeholder has indicated that there is currently no monitoring of the application of technical and organizational measures with regard to the CSP Microsoft.
- The stakeholder does not carry out / does not conduct ongoing data protection risk assessments, including information security risk assessments (ex-post) related to the implementation of cloud computing (CSP Palantir and CSP Microsoft).

**5.2. Which provision(s) of the GDPR (or national laws) does this concern?**

- The principles of Article 24 and Article 32 of the GDPR are not guaranteed, implemented, that, taking into account the nature, scope, context and purposes of the processing, as well as the risks of varying probability and seriousness to the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and be able to demonstrate that the data are processed in accordance with this Regulation. Those measures shall be reviewed and updated as necessary. And the establishment of an adequate level of security shall take into account, in particular, the risks arising from the processing, in

particular the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or unauthorised access to data transmitted, stored or otherwise processed.

**5.3. Explain why this has been an issue for your stakeholders?**

- This caused problems because the stakeholder did not provide the assessments carried out by the CSP, DPIA, did not carry out a risk assessment, did not provide an assessment of the technical and organizational security measures implemented by the CSP, or other evidence based on which it could be said that the CSP ensure an adequate level.

**5.4. What are differences that you have encountered between stakeholders in your Member State?**

- N/A.

**5.5. What are solutions to this issue? Please describe if these solutions are already implemented or potential, and whether this solution is provided by the SA or the stakeholders.**

- A possible solution is to clearly identify, listing the technical and organisational security measures to be implemented by CSP and to carry out a thorough assessment of them, requiring CSP to demonstrate compliance. This decision is provided for by the Lithuanian SA, but has not yet been submitted to the stakeholder, and therefore has not been implemented.

**6. Process to deal with data breaches and notifications (Articles 33 and 34 GDPR).**

**6.1. Name the issue and briefly describe the main issue(s) identified.**

- The agreement between CSP Palantir and the stakeholder did not address the provisions for reporting a personal data breach and cyber incidents and the timing of the response to them.
- The stakeholder has submitted to Lithuanian SA an addendum containing the 2010 SSC CSP Microsoft, which provides for the immediate notification of a personal data breach to the stakeholder, but the exact time is not provided, and also provides that the notice must contain mandatory information under Article 33 of the GDPR, but does not specify exactly what information is to be provided.

**6.2. Which provision(s) of the GDPR (or national laws) does this concern?**

- The principles of Articles 33 and 34 GDPR that, in the event of a personal data breach, the controller shall notify the supervisory authority competent under Article 55 without undue delay and, if possible, within a maximum of 72 hours of becoming aware of the personal data breach, without undue delay and, where possible, within a maximum of 72 hours of becoming aware of the personal data breach, unless the personal data breach would not endanger the rights and freedoms of natural persons and could not be ensured notification to the data subject.

**6.3. Explain why this has been an issue for your stakeholders?**

- The stakeholder's contract does not specify the time when the CSP must notify the stakeholder of a personal data breach, nor does it specify what information is to be contained in the notification.

**6.4. What are differences that you have encountered between stakeholders in your Member State?**

- N/A

**6.5. What are solutions to this issue? Please describe if these solutions are already implemented or potential, and whether this solution is provided by the SA or the stakeholders.**

- Document clearly the procedure for reporting a personal data breach, how long it takes for the CSP to serve the report to the stakeholder on a mandatory basis. Clearly state what information is to be included in the notification. It is possible to prepare a notification form for a personal data breach, which should be completed by the CSP and submitted to the stakeholder. This decision is provided for by Lithuanian SA, but has not yet been submitted to the stakeholder, and therefore has not been implemented.

### **Part III – Actions by the SA**

1. **Have you taken action (i.e. fact-finding exercises, informal contact, prior consultation, investigation) towards any of the stakeholders concerning the use of cloud-based services prior to launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**
  - N/A
2. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (E.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**
  - Firstly, Lithuanian SA are considering correctives measures such as orders without the imposition of administrative fines in order to correct identified issues as soon as possible.

### **Part IV – Other**

1. **What is your general impression of the levels of awareness and compliance of the stakeholders you consulted concerning the use of cloud?**
  - Low level of awareness concerning the use of cloud services, especially where international CSP's involved. No documented consultations with DPO, no contacting SA for advice, no documented decisions not to perform DPIA, poor level of awareness on international transfers. Depending solely on the informational provided by CSPs, not actually verifying it.
2. **Are there any other issues or topics that you would like to flag?**
  - N/A
3. **Are there any leading practices of the stakeholders you have contacted that you would like to share?**
  - N/A

## Part I – Statistics

### 1. How many stakeholders have you contacted within the following categories?

- 3 buyers (strategic vendor managers) for the central government. The explanation of what a strategic vendor manager does is explained in question 4. For the sake of readability for the final report, however, below we refer to these strategic vendor managers as ‘buyers’.

### 2. How many stakeholders have you contacted within the following sectors?

- None specific; the 3 buying departments serve several central government bodies, not from a specific sector, see question 4.

### 3. If you have contacted a buyer, for which sectors does this buyer provides its services:

- No specific sector, see question 4.

### 4. If you have contacted a buyer, and if you have this information, please specify the number of stakeholders this buyer provides services for:

- Unknown. In general, the buyers manage the relation between the Dutch Central Government and the CSPs on behalf of the organisations within the Dutch Central Government. One of the specific tasks of most buyers is to negotiate a legal framework with the CSP in order to facilitate the possible use of products and services by the organisations. The buyers do not buy products and services and do not commit to buy products and services as part of the legal framework. It is the decision of the government body to buy and/or commit to buy products and services from the CSP and as a consequence: to use cloud services.

### 5. What was the initial procedural framework of your action?

- Fact-finding + follow-up actions based on the results.

### 6. How many stakeholders indicated that they use CSPs or are planning to do so in the near future (end of 2022)?

- Not applicable, see question 4. However, we do see that most government organisations in the Netherlands use a CSP. Sometimes in the form of an on-premise solution.

### 7. Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?

- Mainly applications for office productivity functionalities (such as administrative processes, communication and collaboration tools) and/or cloud functionalities (such as computing power, database, storage and identity & access management). However, it is not the buyers’ role to determine for what purposes organisations should use these functionalities.

### 8. For the following commonly identified sectors, please specify if any hyper-scalers<sup>48</sup> are involved (if so please name them) either because they provide the services themselves or because the services are using the infrastructures of these hyper-scalers

---

<sup>48</sup> Hyper-scalers provide cloud services at scale. It refers usually to the big cloud providers (Google, AWS, Microsoft ...) on which other services may also depend

- Central buyers or providers of IT services – Amazon, Google, Microsoft, IBM, SAP, Citrix, Oracle and several smaller CSPs.
- 9. How many stakeholders (AP reads this as: buyers) took the following actions prior to- or during the acquisition of a CSP?**
- Perform a DPIA: **2 out of 3 buyers performed DPIAs or are currently conducting DPIAs. One buyer performed some DPIAs, but not for all CSPs.**
  - Does the DPIA analyse transfers in details (sometimes called DTIA): **Two buyers have done an analysis on transfers or are currently conducting a DTIA, but not for all CSPs. This is because no transfer takes place or no analysis has (yet) been conducted. The Dutch SA cannot say whether all buyers have performed a DPIA/DTIA prior to the acquisition of the CSPs, also because the actual deployment is the choice of an individual government body, not of the buyer.**
  - Contact the DPO for advice: **One buyer notified the DPO, but notes that it performs/commissions umbrella DPIAs, not DPIAs with respect to specific processing of personal data by a specific ministry. The scope of the umbrella DPIAs is a general data protection risk analysis for reuse by the organisations of the central Dutch Government. DPOs of different Dutch Ministries/entities can advise their specific entities falling under their supervision about the implementation or consequences of the umbrella DPIA or DTIA analysis for their individual Dutch governmental entity. Another buyer has asked the DPO for advice and the third buyer did not ask the DPO for advice.**
  - Perform a general risk analysis: **The risk analysis is covered in the DPIA.**
  - Contact the SA for advice: **One buyer consulted the Dutch Supervisory Authority. The outcome was used as an authoritative declaration in the negotiations with Google. It resulted in a further amended contractual document and a remediation plan as agreed with Google. The contract with Google has been signed recently, including the amended provisions as a result of the consultation.**
- 10. How many stakeholders (including buyers) take the following actions during the use of the CSP?**
- Monitoring technical and organisational measures to ensure compliance: **One buyer states that its responsibility is to monitor the CSPs' compliance with the agreed contractual provisions in the framework agreement. For that purpose, it performs technical investigations (such as analysing data flows) on the one hand. On the other hand, it uses third party audits on the implementation of controls in the CSPs operational processes. Another buyer says that there is an intention to coordinate and facilitate the monitoring of the CSPs' compliance with the agreed contractual provisions in the framework agreement. It may perform investigations for that purpose. Whether the buyer actually does so, is unclear. The third buyer has not (yet) taken any actions.**
  - In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g. Schrems II). **One buyer indicates that technical and organisational measures have been proposed as mitigation for the risks as detected within the DTIA/DPIA analysis on Microsoft Teams. On the part of the CSP, certain technical measures have been announced such as the EU Data Boundary and end-2-end-encryption (E2EE) for all calls. The buyer will continue to**

**monitor all developments and guidance from the national supervisory authorities, and update the DTIA whenever that becomes necessary. For the other CSPs a DPIA/DTIA is still in progress. The second buyer has not taken any actions, since the DPIA is still ongoing for a CSP or no transfer takes place. The third buyer is on the verge of concluding an updated legal framework with a CSP and has already signed a Data Processor Agreement with references to international transfers. The buyer mentions that the CSP provides a factsheet with technical & organizational measures as mitigation for the risks from the transfer of personal data to the USA. This only concerns a limited amount of personal data, related to Website visits and Support Data. For other CSPs, there is no indication that any measures have been taken by the buyer.**

- Regular risk assessments: **All buyers have indicated that regular risk assessments are not carried out, since cloud implementation is out of their scope. Several buyers state that monitoring of law developments and required additional provisions is part of their activities. For example, one buyer monitors future legislative developments and if additional investigations or additional provisions are needed because of those developments, action will be taken by them on a general contractual level. There appear to be no set, recurring assessments activities by the buyers.**

## **Part II – Substantive issues**

- A more general comment from the Dutch DPA is that for the use of cloud services, there seems to be a strong focus on international transfer-issues due to Schrems II. However, there are (many) other issues that need to be addressed by public bodies in order to make legitimate use of a processor, for example further processing of personal data, the need to perform a proper (and timely) risk assessment, auditing duties post procurement, properly executing rights of data subjects and informing data subjects.

### **1. Contract with CSPs are ‘repair work’**

- Almost five years after application of the GDPR many public bodies seem to be performing assessments/DPIAs as a form of repairing already existing processing that was not fully compliant with data protection law (not only as a consequence of the Schrems II-ruling). The notion that some sort of assessment/DPIA should be included in procurement policies is rising in The Netherlands.
- Art 28 GDPR.
- Controllers are confronted with a processing of personal data that is not compliant with the GDPR. An ongoing contract has to be revised and negotiations have to take place with the CSP in order to change the terms to be compliant with the GDPR. The ‘repair work’ is often not beneficial for the CSP and as a consequence, the public bodies are dealing with resistance from the CSPs.
- A difference in maturity in dealing with this issue. This goes from full-fledged DPIAs with technical inspections on the data flows to mostly relying on information provided by the CSP.
- Learning from other public bodies and sharing knowledge (internationally).

### **2. Lack of transparency of processed data**

- For customers of CSPs it can be unclear what personal data (telemetry data, data for support, etc.) is processed by the CSP and for what purposes. CSPs also tend to not want to disclose much information, because they see this as confidential information. This can make it difficult for public bodies to adequately fulfil their role as controller.
- Art 5 GDPR.
- Customers of CSPs as controllers may only process personal data in a transparent manner and only for specified and explicit purposes. Without being clear what personal data the CSP processes, customers of CSPs cannot process personal data in a manner compliant with the GDPR. For example; the customer is not able to grant a citizen (data subject) information about the processing of- or access to its personal data.
- Stakeholders do not have a complete overview of the personal data that is being processed and only rely on the general information mentioned in the contracts provided by the CSPs. In the Netherlands, a thorough traffic analysis has been conducted for some CSPs (on behalf of the central buyer) to inspect what telemetry data is collected by the CSP.
- CSPs should give clear and precise information about the personal data that is processed, including for the (specific and explicit) purposes they are processed for. In the Netherlands, some buyers seem to be successful in gaining more transparency from the CSP about this information. A controller should be well-informed by a perceived processor on the processing taking place. A processor should be able to supply this information, for instance based on current customers and his obligation stemming from article 30(2) GDPR. CSPs sometimes unjustly mention that their company trade secrets prevent them from doing so.

### **3. SCCs (module 2 or 3)**

- One buyer has noticed a lot (if not all) CSPs are choosing module 3 of the new SCCs, the “Transfer processor to processor”- module and not the controller to processor-module (module 2).
- Art 46 (1) c GDPR.
- According to the buyer, CSPs sometimes offer the processor-to-processor SCCs instead of the controller to processor SCC as the basis for international transfer. CSPs motivate this by stating that there is an EU representation for the CSP acting as processor via whom the data is transferred outside the EU. However, the representation of a non-EU-based CSP in the EU should not be a criterion when choosing which SCC should be used. Performed factual technical checks of the actual international transfer (DTIA) clearly show that personal data are sent directly from the Dutch government to the US or third countries elsewhere (for example support data), not first through EU member states. Therefore, a controller to processor SCC should be used. The effect of wrongfully offering processor-processor SCCs instead of controller-processor SCCs is that SCCs are used that offer insufficient guarantees for the protection of personal data.
- Because of the significant power imbalance between the contractual parties in question, not every small entity shall be able to contractually agree or disagree with the standard of EU data protection once under pressure of the need for buying products and (software, cloud a.o) services. The Dutch SA has not been able to verify this statement.
- The buyer has chosen the controller to processor-module for international transfer.

#### **4. Insufficient (international) cooperation**

- Publicly available DPIAs, although scarce, do not seem to be widely used by public bodies.
- This leads to public bodies claiming not to know certain issues involving CSPs that they quite easily could, and thus should have known given their size and budget. The same applies for information by other government agencies such as police or intelligence agencies. Their risk assessments can be used as well. For instance, risks related to threats by foreign states looking for personal data could remain unmitigated when this information is ignored.
- Information is being shared but is sometimes focussed on a specific controller. Internationally, information is shared sparsely.
- Make DPIAs available to other public bodies and discuss effective proven ways in dealing with CSPs. The EDPB could also stimulate the publication of DPIAs from public bodies and central buyers (in the final report).

#### **5. Applicable terms in sub processor relationships**

- CSPs can be in a direct relationship with a public body as a supplier, but also in an indirect relationship in its role as a sub processor (for example: a CSP that provides a hosting service to a SaaS service from a different CSP). When a government body already has a contract with that CSP, the terms should also apply when the CSP acts as a sub processor, so that any 'weaker' terms are not applicable.
- Art 28 GDPR.
- In The Netherlands, specific terms are applicable with some large CSPs. As some of these CSPs can also act as a sub processor in other contracts, it is necessary that these terms are also applicable so that the public body is not dependent of any terms with a processor that may not be as detailed so that the public body can perform its role as a controller.
- This was a specific issue raised by a stakeholder, we have not identified whether this issue is also of importance at the other stakeholders.
- In the contracts with the CSPs in question a provision has been added that the terms also apply when the CSP has a contractual relationship with the public body in the role of sub processor.

### **Part III – Actions by the SA**

1. Have you taken action (i.e. fact-finding exercises, informal contact, prior consultation, investigation) towards any of the stakeholders concerning the use of cloud-based services prior to launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).
  - The Dutch Ministry of Justice and Security submitted a request for prior consultation about the possible deployment of Google G Suite Enterprise/Google Workspace by Dutch governmental organisations. We advised against the use of Workspace and Workspace for Education by both parties, because the submitted DPIAs raised fundamental questions about, amongst others, the lack of transparency and the role of processor- and controllership. With our advice, the

negotiating parties reached an agreement with Google. In the explanatory letter sent to the Parliament, the Ministry has stated that all high-risks are mitigated to such an extent that they no longer classify as 'high'.

2. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (E.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

- We keep (informal) contacts with one of the buyers and the CIO department of the central government (CIO Rijk). This is mainly to be updated (on a high level) about the negotiations with CSPs and to retrieve information on the overarching issues regarding the acquisition of CSPs. We also keep contacts with CIO Rijk about the cloud strategy from the Dutch central government and the DPOs, to update them about our findings. We might also be sending a guidance letter towards the central government about the acquisition of CSPs. This could contain some brief feedback on the findings that we have done as part of this coordinated action and also some recommendations towards the future.

#### **Part IV – Other**

1. **What is your general impression of the levels of awareness and compliance of the stakeholders you consulted concerning the use of cloud?**

- It is hard to give a general impression, as we have seen that the level varies greatly between the 3 buyers that we have consulted. For one buyer the level appears to be very high. We see that a lot of time and resources (including by consulting external organisations) are invested to raise the compliance level in contracts with the large CSPs; this is not a maturity level that every organisation can achieve (on its own). On the other hand, we have also seen a buyer that gave very vague information and does not seem to have the expertise and resources available to achieve a high level of awareness/compliance. Fortunately, we do see that a certain level of cooperation is taking place between the buyers (and DPOs), which raises the overall level.

2. **Are there any other issues or topics that you would like to flag?**

- Cooperation is key in negotiating contracts with large CSPs; in the Netherlands, buying organisations are taking a more important role (also in the educational sector). We believe that SAs can contribute to the overall level of compliance by encouraging this type of cooperation. This cooperation should take place on both on a national level (e.g. within a certain sector) and on an international level (publishing DPIAs and learning from contractual agreements made by other parties).
- We would also like to quote the following answer we have received from one of the buyers regarding the experiences performing a DPIA:

*"A positive experience with performing a DPIA is the leverage which is created if data protection risks are identified. We clearly benefit from the harmonisation of European (privacy) laws, since the risks identified in the DPIA can be applied by all European organisations that use the services of the same CSP. CSPs are aware that assessed risks are potentially blocking their business in the EU. A negotiation about the assessed risk-mitigation also opens the door for related issues like liability in case of breaching the DPA. For the CSPs, the negotiations with [buyer] also offer added value, because they benefit from input on*

*specific mitigation measures, and by being able to confidentially discuss obstacles and timeframes to implement such mitigation measures.*

*Negative experiences are the huge investments in technical, legal and CSP management capacity. [Buyer] is able to organise this on a central government level, but it still requires a lot even from a central government organised team. The financial investments are also huge, because external experts are needed during the whole process of investigation, negotiations and contracting with CSPs, together with at least 3 or more civil servants. Added to this is the relatively new requirement of performing a DTIA, for which even more capacity is needed. The results of [buyers] work are only applicable to civil servants, related (external) contract workers and Dutch persons who are interacting with employees under a central government license. Private sector organisations and consumers/citizens are not covered by the results of [buyers] work. Because the negotiated legal frameworks need proper management, additional investments (e.g. technical verification, audits, DPIA's) are required on an ongoing basis."*

- The lack of a clear cloud national strategy gives room for public bodies to make their own individual decisions. Decisions including why, when and how a CSP is being contracted. While, in individual cases, it can be inefficient to start thinking about a private cloud, this can become much more feasible from a countrywide perspective. A countrywide cloud strategy could include a timeline for development of a national, or European, cloud infrastructure (gradually) developing from an IaaS to a SaaS-solution. This will also impact the decision on the necessity of choosing a non-EU CSP in the years to come.

### **3. Are there any leading practices of the stakeholders you have contacted that you would like to share?**

- Yes, we would like to share the following best practices from one of the buyers:
  - Conducting ‘umbrella’ DPIAs and DTIAs in which the ‘default’ processing of the cloud platform is technically investigated in several defined use cases that (governmental) organisations can use for their own assessment.
  - Publishing DPIAs and DTIAs on a publicly accessible website.
  - An approach that contractually guarantees the processing of personal data only on documented instructions. Furthermore, all possible purposes are explicitly authorized in the documented instructions. These purposes are included to ensure that processing does not go beyond what is necessary to deliver the service, keep the services secure and up to date.
- With regards to purpose limitation, the buyer takes the following approach:
  - There is a limitative list of authorized purposes for which the processor may process personal data, for example: providing the service, keeping it up to date and secure.
  - The buyer explicitly authorises the CSP to ‘further’ process some personal data for narrowly defined purposes. These purposes are defined in an exhaustive list in the (amended) data processing agreement, which is part of the legal framework. The purposes are related to legitimate business purposes for which the CSP necessarily has to act as the sole controller, such as invoicing, accounting, fraud detection and technical infrastructure forecasting.

- To further limit processing of personal data outside the scope of authorized purposes, the instructions include certain prohibited purposes. This means that the CSP for example may not use personal data for profiling, advertising or analytics. This approach is an extra measure to ensure that a CSP cannot use the data for all things he renders necessary as a controller.
- Initially, the DPIAs on both Microsoft and Google services concluded that factually the organisations and the CSP were joint controllers, and flagged the lack of control over the data processing (due to the lack of transparency and lack of a joint controller agreement) as a high risk. After the negotiations about mitigating measures, the CSPs are no longer joint controllers.
- Verification of the CSP's compliance with the agreed legal framework is also managed by the buyer. This means that, with regard to the data processing agreement, the buyer selects certain services to audit in a technical way (technical verification against contractual provisions) combined with audits with respect to the CSP internal processes (and the controls thereof).
- The processor is allowed to engage a sub processor. For the engagement of a sub processor that is related to essential or core services, the notification of engagement is sent substantially sooner, as it is possible that the sub processor will gain access to customer content data.
- The buyer routinely carries out technical verification analyses with the assistance of qualified third parties. For example, the buyer verifies whether services indeed comply with a committed security level. Moreover, specific security measures and frameworks are specified in the legal framework. It should be noted that the customer in such a scenario is largely dependent on the cooperation on the part of the vendor. This is of great importance, as there are no other means to verify any obligation without adequate cooperation of the vendor. The buyer always includes specific extensive audit provisions in the legal framework, to prevent possible conflicts when verifying compliance with external auditors.

**Part I – Statistics**

**1. How many stakeholders have you contacted within the following categories?**

- Ministry of the central government
- Independent public body of the central government **(3)**
- Buyer for the central government
- Publicly-owned company acting as a processor for several central public bodies
- Ministry of the regional government
- Independent public body of the regional government
- Buyer for the regional government
- Publicly-owned company acting as a processor for several regional public bodies
- Other, please specify: public buyer for public health sector **(1)**

**2. How many stakeholders have you contacted within the following sectors?**

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government **(2)**
- Economic affairs
- Education
- Finance
- Health **(1)**
- Infrastructure
- Employment
- Justice
- Tax
- Other, please specify: social security **(1)**

**3. If you have contacted a buyer, for which sectors does this buyer provides its services:**

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government
- Economic affairs
- Education
- Finance
- Health **(1)**
- Infrastructure
- Employment
- Justice
- Tax
- No specific sector
- Other, please specify
- 

**4. If you have contacted a buyer, and if you have this information, please specify the number of stakeholders this buyer provides services for:**

- 120.000 in 1900 .locations

**5. What was the initial procedural framework of your action?**

- Fact finding
- Fact finding + determining follow-up action based on the results
- New investigation<sup>49</sup> X
- Ongoing investigation

**6. How many stakeholders indicated that they use CSPs or are planning to do so in the near future (end of 2022)?**

- All of the stakeholders investigated: 4

**7. Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?**

- Internal organisation (office suites, internal communication, HR, etc.) - (4)
- Exercise of public functions (services to citizens, processing citizen's data, etc.) – (1)

**8. For the following commonly identified sectors, please specify if any hyper-scalers<sup>50</sup> are involved (if so please name them) either because they provide the services themselves or because the services are using the infrastructures of these hyper-scalers: No**

- Health
- Finance
- Tax
- Education
- Central buyers or providers of IT services

**9. How many stakeholders took the following actions prior to- or during the acquisition of a CSP?**

- Perform a DPIA (0)
- Does the DPIA analyse transfers in details (sometimes called DTIA) (0)
- Contact the DPO for advice (2)
- Perform a general risk analysis (3)
- Contact the SA for advice (0)

**10. How many stakeholders (including buyers) take the following actions during the use of the CSP?**

- Monitoring technical and organisational measures to ensure compliance: **none**
- In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g. Schrems II): **none**
- Regular risk assessments: **none**

## **Part II – Substantive issues**

**1. No direct contract with the CSP and no negotiation of the terms**

- The absence of a direct contract with the CSP is a common issue to all stakeholders, and it seems that stems from the way the most known CSP conduct their business. This is a problem, because there is no possibility of negotiating the terms of the contract, in particular taking advantage of a

---

<sup>49</sup> making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred

<sup>50</sup> Hyper-scalers provide cloud services at scale. It refers usually to the big cloud providers (Google, AWS, Microsoft ...) on which other services may also depend

broad expected use of the services, or of the fact that it is a public body directly linked to the central government with a higher negotiating power. In addition, it becomes more difficult to have tailor-made rules covering the contract and providing an adequate reply to certain legal requirements. Somehow, this limits the choice of a processor that offers guarantees, as required by Article 28(1) GDPR. There is a clear inversion of roles, when the processor is not in a position to choose and to instruct the (sub) processor. The processor is just an intermediary and it only artificially performs the tasks envisaged by the GDPR and entrusted by the controllers.

- The solution is to find CSPs that are willing to negotiate directly and that submit themselves to the public procurements for their services, without using proxy (national) companies to make the contracts.
- Furthermore, some controllers rely on the terms of the contract with the intermediary companies (processors) to demand certain legal conditions to meet data protection requirements (obligation of result) that objectively cannot be ensured by those processors, as they are in no position to give further instructions to the sub(processors) that actually provide the cloud services. This having into account that the CSPs at stake are the so-called Internet giants. It is indeed a false indication of compliance.

## **2. No clear allocation of roles among the public bodies**

- The public bodies launching the procurement for cloud services and entering into contracts are not, in some cases, the actual controllers. Some IT public institutes assume the role of controllers, when making the decisions on the means and on the purposes of the processing without consulting the 'owners of the data', i.e. who by virtue of their legal competences are the effective controllers and employers of the human resources using the cloud services. Even if in some situations a joint controllership would be applicable and the most suitable solution, such arrangement is not in place pursuant Article 26 GDPR. This excludes the effective controllers of the decision-making process and, thus, of their responsibilities. The pandemic crisis led to a quick recourse to cloud services because of teleworking, without contemplating all the pros and cons of such solutions. Furthermore, with the confinement, there was an increased need of public services available remotely and online by citizens.

## **3. Lack of DPIA**

- None of the stakeholders carried out a DPIA to assess the impact of the choice of having cloud services and the extent of the use of such services.
- This is in breach of Article 35 (1) GDPR. This shows that controllers are not fully aware of their data protection obligations. Moreover, the lack of DPIA did not allow the identification of risks and the adoption of appropriate measures to mitigate such risks or to decide on alternative ways to get the needed services. Two stakeholders performed some risk analysis, in very general terms, what did not permit to have a thorough overview of the essentials. In addition, data protection officers were not properly involved from the outset in the projects; thus, they did not have the opportunity to convey their advice to the controller.

## **4. Failures in the contract with processor**

- The DPA identified failures in the data processing agreements required by Article 28 GDPR. The controllers entered into contracts with (intermediary) processors, but not all legal conditions were met. The Service Level Agreement (SLA) was in fact the core of the contract. No negotiating terms, as explained in Issue 1, or imposed limitations on data processing. However, all contracts contain

reversibility/termination control clauses. Only one stakeholder incorporated clauses on data breaches.

- Another relevant aspect is the fact that the insertion of some requirements in the contract (like, location of the data) are not implemented in practice or monitored whatsoever by the stakeholder, since the (intermediary) processor is not in a position to ensure the compliance with this term of the contract. On the other hand, the stakeholder (controller) does not take any other steps to verify or guarantee that the data is indeed in the EU and that is not accessed by third country authorities. This is connected with the following issue 4.

#### **5. Insufficient assessment towards the requirements on international transfers**

- The stakeholders show to have insufficient awareness of the legal framework on international transfers, in particular after the Schrems II judgement. Some stakeholders managed to secure in the contracts with the (intermediary) processor the condition that the personal data stays within the EU. But at the same time, they accept standard contractual clauses as a valid mechanism for international transfers. No assessment was made on the factual conditions of the data processing, including transfers to third countries (e.g. via telemetry or via direct governmental access to data centres located in the EU). Misinterpretation that a simple clause in the contract requiring the data to be located in Portugal or within the EU is enough to ensure that data is no further transferred. Therefore, no assessment of the third country is done or supplementary measures requested or adopted.

#### **6. Lack of awareness in relation to telemetry and diagnosis data**

- The stakeholders were not aware of the processing of data for purposes of telemetry and of the respective legal obligations. No requirements were made or negotiated, in order to apply the principle of data minimisation (Article 5(1) (c) GDPR); the principle of data protection by design and by default (Article 25); security measures (article 32). It was evident that some of this data was used by the stakeholders, but in some limited extent, in particular in what audit logs are concerned. In general, this kind of data is not perceived as personal data subject to GDPR requirements by all stakeholders.

#### **7. Lack of monitoring of compliance**

- The stakeholders do not perform any kind of check on compliance or monitoring of the actions carried out by processors, in clear breach of Article 28. This is a common conclusion from the investigation on the four stakeholders. There are no procedures in place in case of data breaches, especially because the cloud solutions are seen as more secure solutions than other alternatives. Yet some cyberattacks already known target or explore security breaches in the processors that disclose users' credentials and enable an entry into the organisations and get access to their infrastructures.

### **Part III – Actions by the SA**

1. **Have you taken action (i.e. fact-finding exercises, informal contact, prior consultation, investigation) towards any of the stakeholders concerning the use of cloud-based services prior to launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

- No. The Coordinated enforcement action was the starting point for the inspection of 4 stakeholders at national level.
- 2. What action(s) are you planning to undertake based on the results of this coordinated action, if any? (E.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**
- No decision was taken so far, as the inspection reports are yet to be finalised. Then, the data protection authority will issue a decision, which cannot be anticipated at this point; however, the minimum outcome will be recommendations to the stakeholders. But based on similar situations, most likely some corrective measures will be applied.

#### **Part IV – Other**

- 1. What is your general impression of the levels of awareness and compliance of the stakeholders you consulted concerning the use of cloud?**
- In general, it is our impression that there was a certain level of awareness on the risks associated with cloud services, in particular related to international transfers, as this has been an issue with some media coverage after the Schrems II and the DPA decisions; hence, the requirement on the location of data within the EU. However, in practical terms, the solutions adopted are clearly insufficient to tackle the issue. In addition, under the pressure of finding options during the pandemic crisis and the need to address teleworking and online access by citizens to public services with urgency, no prior risks assessments (such as DPIAs) were carried out or the high involvement of DPOs. It could also be underlined that the adoption of cloud services solutions is a result of public bodies being understaffed in IT experts. The cloud solutions require much less in-house manpower to manage the infrastructures.
- 2. Are there any other issues or topics that you would like to flag?**
- The fact that there is no direct contract or negotiation with the CSP (in case of big multinational companies) hinders the proper compliance of Article 28 and the other GDPR obligations.
  - It should be highlighted though that the use of CSP is not applicable to the core activities of the public bodies, i.e. not involving data processing of a large universe of data subjects. The stakeholders concerned have their own data centres and infrastructures, where the data is stored, what is very positive. The cloud services mostly used relate to active directories, email functionalities, videoconferencing and office productivity tools.
  - Conversely, there is no specific training to staff on how to use these tools appropriately, in particular preventing from processing personal data of citizens using the cloud storage capabilities, within the daily activities.
- 3. Are there any leading practices of the stakeholders you have contacted that you would like to share?**
- No

## Part I – Statistics

### 1. Which stakeholders have you contacted under the coordinated action?

- The Swedish Tax Agency
- Enforcement Authority (government agency that deals with debts)
- The Swedish Social Insurance Agency
- The Swedish Pensions Agency
- The Swedish Companies Registration Office
- The Swedish Public Employment Service
- The Swedish Board of Student Finance
- The Agency for Digital Government
- The Swedish Civil Contingencies Agency
- The Swedish Transport Administration
- The Swedish Mapping, cadastral and land registration authority

### 2. How many stakeholders have you contacted within the following categories?

- Ministry of the central government: **0**
- Independent public body of the central government: **11**
- Buyer for the central government: **0**
- Publicly-owned company acting as a processor for several central public bodies: **0**
- Ministry of the regional government: **0**
- Independent public body of the regional government: **0**
- Buyer for the regional government: **0**
- Publicly-owned company acting as a processor for several regional public bodies: **0**
- Other, please specify

### 3. How many stakeholders have you contacted within the following sectors?

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government: **1**
- Economic affairs
- Education
- Finance: **3**
- Health
- Infrastructure: **3**
- Employment: **1**
- Justice
- Tax: **1**
- Other, please specify: **3**

### 4. If you have contacted a buyer, for which sectors does this buyer provides its services?

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government
- Economic affairs
- Education

- Finance
- Health
- Infrastructure
- Employment
- Justice
- Tax
- No specific sector
- Other, please specify

**5. If you have contacted a buyer, please specify the number of stakeholders this buyer provides services for**

**6. What was the initial procedural framework of your action?**

- Fact finding X
- Fact finding + determining follow-up action based on the results
- New investigation
- Ongoing investigation

**7. How many stakeholders indicated that they use CSPs or are planning to do so in the near future (end of 2022)?**

- We received 7 answers, all of them said they use CSPs.

**8. Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?**

- Internal organisation (office suites, internal communication, HR, etc.)
- Exercise of public functions (services to citizens, processing citizen's data, etc.)
  
- **Answer:** Answers were not very clear, but it seems like all of them are mainly using CSPs for internal organisation.

**9. For the following commonly identified sectors, please specify if any hyper-scalers are involved (if so please name them)**

- Health
- Finance
- Tax
- Education
- Central buyers or providers of IT services

**10. How many stakeholders took the following actions prior to- or during the acquisition of a CSP?**

- Perform a DPIA: **6/7 (However, they do not seem to be performing DPIAs for every single acquisition, but when a DPIA is required.)**
- Does the DPIA analyses transfers in details (sometimes called DTIA): **7/7**
- Perform a general risk analysis: **7/7**
- Contact the DPO for advice: **7/7**
- Contact the SA for advice: **0/7**

**11. How many stakeholders (including buyers) take the following actions during the use of the CSP?**

- Monitoring technical and organisational measures to ensure compliance: **6/7**

- In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g. Schrems II): **4/7**
- Regular risk assessments: **4/7**

## **Part II – Substantive issues**

- **Name the issue and briefly describe the main issue(s) identified.**
- **Which provision(s) of the GDPR (or national laws) does this concern?**
- **Explain why this has been an issue for your stakeholders?**
- **What are differences that you have encountered between stakeholders in your Member State?**
- **What are solutions to this issue? Please describe if these solutions are already implemented or potential, and whether this solution is provided by the SA or the stakeholders.**

### **1. Contract with the CSP**

- Answers regarding the roles differs between different stakeholders, some (4/7) say the authority is the controller and the CSP is processor, some answers are really short and one answer indicates that there is a joint controllership with the CSP.
- Art 24, 26
- The answers do not really clarify.
- More guidance and maybe inspections regarding the responsibility for organisations when using CSPs.

### **2. International transfers and access by foreign public authorities**

- 4/7 authorities do not really answer the question about if personal data is being transferred to third countries. 3/7 seem to be transferring data to some extent or at least in a few cases. We can assume that transfers are being made at least occasionally even in the cases where they did not answer. However, regarding which tool of transfer the transfers are based on, 4/7 did not answer and only 1/ mentioned SSCs and 1/7 mentioned art 49. Conclusion in transfers are being made without an applicable tool of transfer.
- Art 44-49
- Doesn't say but probably because the difficulty to use US CSPs and how to deal with that situation, and the difficulty to perform TIAs.
- Larger problems for smaller organisations who do not have the financial resources to hire staff who have deeper knowledge about both technical and legal issues, also harder for them to negotiate with CSPs.
- Guidance is always valuable, maybe inspections are more efficient when it comes to making the CSPs change and create services that are compliant with the GDPR.

### **3. Telemetry data**

- Only 1/7 authorities are answering that they do investigate whether telemetry data is being collected by the CSP. 6/7 are not answering or answer that they do not know. Follow up questions are not really being answered, or the answer is that they don't' know.
- Responsibility issue, art 24.
- Doesn't say but there is probably not very much awareness about collection of this kind of data, authorities are probably focusing mainly on 'direct' personal data.
- Hard to say, there seem to be a lack of awareness among all the authorities in this case.
- Maybe more guidance as a start, since the stakeholders seem to lack basic knowledge about this.

#### **4. Compliance**

- 6/7 stakeholders claim they do monitor the implemented technical and organisational measures, but during which circumstances they do that differs. However, only 3/6 monitor if the CSP perform risk assessments.
- Art 24, 32
- Does not say but monitoring risk assessments probably demands a higher level of awareness by the controller, than monitoring TOMs. Some stakeholders probably have not reached that level (yet).
- Hard to say, but authorities with more experience in using CSPs are probably most likely to have knowledge about the need to monitor risk assessments.
- Maybe guidance as a start, some stakeholders seem to lack awareness about this, but inspections might be needed as well further on.

### **Part III – Actions by the SA**

1. Have you taken action (i.e. fact-finding exercises, informal contact, prior consultation, investigation) towards any of the stakeholders concerning the use of cloud-based services prior to launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).
  - Answer: No.
2. What action(s) are you planning to undertake based on the results of this coordinated action, if any? (E.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)
  - Answer: We have written a report regarding the national investigation in November 2022.

### **Part IV – Other**

1. What is your general impression of the levels of awareness and compliance of the stakeholders you consulted concerning the use of cloud?
  - Answer: Pretty good awareness regarding the process for acquisition, regarding the international transfers and processing of telemetry data not so good. We did however send the questionnaire to big authorities who we believe have a lot of experience in using cloud-based services, the level of awareness is probably lower among authorities in general in Sweden.

# SI SA

Slovenian SA (Information Commissioner of the Republic of Slovenia)

## Part I – Statistics

### 1. How many stakeholders have you contacted within the following categories?

- Ministry of the central government: **1**
- Independent public body of the central government: **0**
- Buyer for the central government: **0**
- Publicly-owned company acting as a processor for several central public bodies: **0**
- Ministry of the regional government: **0**
- Independent public body of the regional government: **0**
- Buyer for the regional government: **0**
- Publicly-owned company acting as a processor for several regional public bodies: **0**
- Other, please specify: **3 public research institutes**

### 2. How many stakeholders have you contacted within the following sectors?

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government
- Economic affairs
- Education: **4**
- Finance
- Health
- Infrastructure
- Employment
- Justice
- Tax
- Other, please specify

### 3. If you have contacted a buyer, for which sectors does this buyer provides its services:

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government
- Economic affairs
- Education
- Finance
- Health
- Infrastructure
- Employment
- Justice
- Tax
- No specific sector
- Other, please specify
- Not applicable

### 4. If you have contacted a buyer, and if you have this information, please specify the number of stakeholders this buyer provides services for:

- 5

5. **What was the initial procedural framework of your action?**
- Fact finding
  - Fact finding + determining follow-up action based on the results
  - New investigation<sup>51</sup>
  - Ongoing investigation
6. **How many stakeholders indicated that they use CSPs or are planning to do so in the near future (end of 2022)?**
- 1
7. **Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?**
- Internal organisation (office suites, internal communication, HR, etc.) : 1
  - Exercise of public functions (services to citizens, processing citizen's data, etc.): 1
8. **For the following commonly identified sectors, please specify if any hyper-scalers<sup>52</sup> are involved (if so please name them) either because they provide the services themselves or because the services are using the infrastructures of these hyper-scalers**
- Health
  - Finance
  - Tax
  - Education: Microsoft 356
  - Central buyers or providers of IT services
9. **How many stakeholders took the following actions prior to- or during the acquisition of a CSP?**
- Perform a DPIA: 0
  - Does the DPIA analyse transfers in details (sometimes called DTIA): 0
  - Contact the DPO for advice: 0
  - Perform a general risk analysis: 0
  - Contact the SA for advice: 0
10. **How many stakeholders (including buyers) take the following actions during the use of the CSP?**
- Monitoring technical and organisational measures to ensure compliance: 0
  - In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g. Schrems II) : 0
  - Regular risk assessments: 0

## Part II – Substantive issues

### 1. **LACK OF CONDUCTING DPIA**<sup>53</sup>

---

<sup>51</sup> making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred

<sup>52</sup> Hyper-scalers provide cloud services at scale. It refers usually to the big cloud providers (Google, AWS, Microsoft ...) on which other services may also depend

<sup>53</sup> the issue identified is based solely on the response of one questionnaire since only one participant stated that they use a CSP

- Despite the many risks that the use of cloud services in the public sector has on the protection of personal data, we gathered from the responses of the participating stakeholder that uses a CSP that a DPIA has not been conducted, neither before the intended processing itself, nor in the process of stipulating contractual provisions.
- Article 35 and 36 GDPR; relevant recitals of the GDPR: (75), (76), (77), (84), (90), (91), (92), (93), (95).
- Due to the lack of DPIA being conducted by the controller, we see challenges in terms of controller not fully understanding all the obligations regarding personal data protection and the importance of DPIA as a tool to mitigate various personal data processing risks.
- One stakeholder stated that they use a CSP and has not conducted DPIA.
- SI SA has already published general guidelines on the implementation and importance of data protection impact assessment ([https://www.iprs.si/prirocniki\\_smernice/Smernice\\_o\\_ocenah\\_ucinka.pdf](https://www.iprs.si/prirocniki_smernice/Smernice_o_ocenah_ucinka.pdf)), which will be reviewed in more detail and supplemented according to the specifics of the processing resulting from the use of cloud services in the public sector. In addition, in accordance with the (national or EDPB) findings, targeted trainings on this topic could additionally be conducted, focused on a clearly defined circle of organizations in the public sector that implement or use such services in their work.

## **2. LACK OF SUFFICIENT GUARANTEES FORSEEN IN REGARDS TO ENSURING APPROPRIATE TECHNICAL AND ORGANISATIONAL MEASURES**

AND

## **3. MONITORING OF THE IMPLEMENTED TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING SECURITY MEASURES OF THE CSPS<sup>54</sup>**

- Controllers often do not have all the information about how a certain cloud provider ensures some essential elements of personal data security, such as the traceability of processing, the deletion of personal data after the purpose of processing has been fulfilled, and information about the actual locations of personal data etc. In such situations, it is difficult for personal data controllers to carry out adequate risk analysis before deciding to use these cloud services. Based on the response from one stakeholder that uses a CSP we identified a lack of sufficient guarantees in relation to assurances about (adequate security, technical and organisational measures that are being implemented by the cloud service provider).
- Article 32 GDPR; Article 24 & 25 of Personal Data Protection Act (ZVOP-1);
- Based on the response of one stakeholders, we note a lack of implementation of technical or organizational measures to mitigate risks and establish adequate safeguards prior to the processing carried out when using cloud service providers. Additionally there is no monitoring mechanism provided or used by the controllers. One stakeholder states that they only perform the measure of sporadic inquiry about the physical location of the data.
- No substantial differences have been noticed.

---

<sup>54</sup> the issue identified is based solely on the response of one questionnaire since only one participant stated that they use a CSP

- Given the lack of basic knowledge in the field of personal data protection, alongside the diversity and complexity of the risks that the use of this type of technology has on the protection of personal data, it would be necessary to further educate the relevant public and implement various preventive mechanisms (such as additional guidelines, training...), which would encourage the awareness of these controllers and ensure greater compliance in this area.

#### **4. UNCLEAR ROLE OF THE PARTIES<sup>55</sup>**

- Controllers in general often accept the general conditions of the use of services, where the controller of personal data is often a party with less bargaining power, who can usually only accept or reject the general conditions of the use of services submitted to him by the provider of cloud computing services, even though the controller of personal data is the one who determines the purposes, circumstances and means of processing and the required level of protection of personal data. Due to the disproportionate balance of power it is crucial that there is a clear determination of roles done by the controller and by the processor. The controller must adequately establish its role in the processing activities and its relation to the cloud services provider, while the contract must specify the controls regarding the processing of the processor and specify the risk mitigating measures within the contract;
- Articles 24, 26 - 29 GDPR, Article 11 Personal Data Protection Act (ZVOP-1);
- It follows from the responses of the stakeholder that uses the CSP that they are not aware of the content of the contract, which was accepted on their behalf by the central buyer of the cloud services of the specific provider, nor that this contract contained any essential provisions on ensuring compliance of personal data processing with relevant regulations in the field of personal data protection.
- No substantial differences have been noticed.
- Given the controller's lack of basic knowledge in the field of personal data protection, additional training might be necessary. In addition, it should be noted that the participating stakeholder did not involve a DPO when determining or accepting the relevant contract with the CSP. With that in mind, the role of the DPO when determining such processing activities based on a contract should be emphasized.

#### **5. LACK OF AWARENESS ON INTERNATIONAL PERSONAL DATA TRANSFERS<sup>56</sup>**

- Specific difficulties in ensuring the expected level of protection of personal data also arise from the related issues of exporting personal data to third countries that (do not) provide the same levels of personal data protection as the home jurisdiction. This especially applies when the personal data that is being transferred is by a public sector organisation and/or large in volume.
- Chapter V. of GDPR, Article 63-71 ZVOP-1.

---

<sup>55</sup> the issue identified is based solely on the response of one questionnaire since only one participant stated that they use a CSP

<sup>56</sup> the issue identified is based solely on the response of one questionnaire since only one participant stated that they use a CSP

- Since the answers were quite limited in scope and in its content, it can be deducted that there is a lack of awareness on the problematics and obligations of using a provider where the rules of international persona data transfer applies.
- No substantial differences have been noticed.
- SI SA has already written quite a vast number of non-binding opinions and included the topic of international data transfers in many of our general guidelines. Based on results we will analyse whether there is a need for a specific training, promotion of our guidelines and/ or other preventive mechanism is necessary.

### **Part III – Actions by the SA**

1. **Have you taken action (i.e. fact-finding exercises, informal contact, prior consultation, investigation) towards any of the stakeholders concerning the use of cloud-based services prior to launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**
  - Before the implementation of our joint coordinated action, SI SA issued a number of non-binding opinions on the obligations of controllers regarding their use of cloud services. We emphasized the importance of transparency and available information to individuals, the controller's responsibility for ensuring adequate technical and organizational measures for data security, and the importance of conducting the data protection impact assessment to evaluate the effects on the protection of personal data. In addition to the aforementioned actions above, we also issued general guidelines on cloud computing, where we first defined the main features and concepts of cloud computing and described in more detail the obligations of controllers in relation to the export of personal data to third countries, adequacy of contractual provisions, security of personal data processing, etc. As part of the mentioned guidelines, we have also created a checklist for checking the controller's compliance when using cloud-computing services concerning personal data protection requirements.
2. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (E.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**
  - We will continue to issue non-binding opinions and guidelines on this topic by taking into the account the findings of this coordinated action, while also emphasizing the importance of a consistent and careful approach to the introduction and use of cloud service provides in the public sector. We will consider potential updates to our (already existing) guidelines on cloud computing. Based on the findings we will also consider if further enforcement measures will be applied.

### **Part IV – Other**

1. **What is your general impression of the levels of awareness and compliance of the stakeholders you consulted concerning the use of cloud?**
  - The stakeholders to whom we addressed the respective questionnaire demonstrated limited knowledge of both understanding (i) what cloud services are (ii) their obligations in connection

with the protection of personal data arising from their use. Based on four obtained questionnaires, we received an answer of only one stakeholder where they confirmed the use the cloud service provider both for organizational work within the organization and for the implementation of their public function. The other stakeholders confirmed to us that they do not use cloud services, outside of the use of providers such as Zoom and Cisco, although some use for example Google Analytics on their website. In conclusion, we also note the lack of both the inclusion of DPOs in the process of adopting contractual provisions as well as the lack of conducting the DPIA, as a preventive tool in identifying the risks that a concrete processing may have on the right to the protection of personal data. In addition, it can be deduced from the answers that the stakeholders are rather unaware of the problems and risks of using such technologies for the rights of individuals and the problem of the transfer of personal data to third countries.

2. **Are there any other issues or topics that you would like to flag?**
3. **Are there any leading practices of the stakeholders you have contacted that you would like to share?**

# SK SA

## Part I – Statistics

### 1. How many stakeholders have you contacted within the following categories?

- Ministry of the central government: **2**
- Independent public body of the central government: **3**
- Buyer for the central government
- Publicly-owned company acting as a processor for several central public bodies
- Ministry of the regional government
- Independent public body of the regional government
- Buyer for the regional government
- Publicly-owned company acting as a processor for several regional public bodies
- Other, please specify

### 2. How many stakeholders have you contacted within the following sectors?

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government: **1**
- Economic affairs
- Education
- Finance: **1**
- Health
- Infrastructure: **1**
- Employment
- Justice
- Tax
- Other, please specify – audit, statistics

### 3. If you have contacted a buyer, for which sectors does this buyer provides its services:

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government: **Probably yes, the Ministry negotiates framework documentation and each stakeholder must conclude its own contract using this framework documentation. (The word “probably” is just solely for the reason that in order to expressly confirm the factual situation, more evidence shall be gathered (as we did not exactly ask for this question in the questionnaires).**
- Economic affairs
- Education
- Finance
- Health
- Infrastructure
- Employment
- Justice
- Tax
- No specific sector
- Other, please specify

**4. If you have contacted a buyer, and if you have this information, please specify the number of stakeholders this buyer provides services for:**

- We have not demanded for this information.

**5. What was the initial procedural framework of your action?**

- Fact finding
- Fact finding + determining follow-up action based on the results
- New investigation<sup>57</sup>
- Ongoing investigation

**6. How many stakeholders indicated that they use CSPs or are planning to do so in the near future (end of 2022)?**

- 5

**7. Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?**

- Internal organisation (office suites, internal communication, HR, etc.): 5
- Exercise of public functions (services to citizens, processing citizen's data, etc.): 3

**8. For the following commonly identified sectors, please specify if any hyper-scalers<sup>58</sup> are involved (if so please name them) either because they provide the services themselves or because the services are using the infrastructures of these hyper-scalers**

- Health
- Finance: 1
- Tax
- Education
- Central buyers or providers of IT services

**9. How many stakeholders took the following actions prior to- or during the acquisition of a CSP?**

- Perform a DPIA
  - Does the DPIA analyse transfers in details (sometimes called DTIA)
  - Contact the DPO for advice
  - Perform a general risk analysis
  - Contact the SA for advice
- 
- Answer: 0

**10. How many stakeholders (including buyers) take the following actions during the use of the CSP?**

- Monitoring technical and organisational measures to ensure compliance
- In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g. Schrems II).
- Regular risk assessments

---

<sup>57</sup> making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred

<sup>58</sup> Hyper-scalers provide cloud services at scale. It refers usually to the big cloud providers (Google, AWS, Microsoft ...) on which other services may also depend

- Answer: 0

## Part II – Substantive issues

### 1. At pre-contractual phase

- Based on the answers provided in the questionnaires, we noticed lack of knowledge about the fact that the services used by stakeholders are identified as cloud services. They seem not to take into account GDPR rules not only during pre-contractual phase but also during the implementation phase. Another principal issue resulting from the answers is that the answering body did not even understand technology or law at stake. Consequently, answers provided were not factually correct – people with technical background do not understand legal questions, and vice-versa, people with legal background answered the questionnaire incorrectly, but in line with what the GDPR is supposed to require (however, the practice is obviously different).
- N/A
- We have received contradicting answers, Stakeholder responsible for the framework of contractual relationships for public bodies declared that they use only one type of cloud service and other Stakeholder claimed that they are using other type of cloud service but contractual relationships are procured by the former Stakeholder and that they do not have power to change the contractual relationship.
- We have found out that the level of knowledge and compliance practice with data protection rules are low. We have not received any answer from the concerned public body that would obviously provide evidence that the GDPR rules are taken into account at pre-contractual phase. The main difference is that some stakeholders said that they use only one type of service cloud provider. However, we did not receive convincing information that would confirm that the GDPR rules are taken into account prior to conclusion of contractual relationship even with the one cloud provider. In one case, the stakeholder stated that they are working on the amendments to the contract which will cover data protection or that there is no controller-processor contract and only the business contract presuppose conclusion of controller-processor contract which has not been concluded yet.
- With regard to the basic knowledge about the GDPR requirements of the stakeholders involved in the questionnaire, we are considering how to improve data protection knowledge within their employees. Currently, we will propose stakeholders to organise trainings about the cloud related topics targeting data protection obligations, which should be provided by their Data Protection Officers and send evidence about this specific trainings to SA. Another solution, which we plan to initiate, based on the analysed questionnaires is to create follow-up letter that will highlight the most obvious discrepancies for each individual stakeholder involved in our survey. The aim is to stay in contact and request regular information about implementation of GDPR processes with their cloud provider. These letters will also include obligation of stakeholders to communicate with their Data Protection Officer in case of any cloud related topic issues.

## **2. Lack of documentation**

- The stakeholders seem to have no knowledge that they are obliged to conclude Art.28 (3) contract.
- Some stakeholders do not have or asked for the Data Protection Impact Assessment. No stakeholders in question were able to provide us with the DPIA. We have received only one document focusing solely on data protection, however it is not clear whether it is legally binding document neither it is sure who is obliged by it. This document has general nature and is unclear in data protection clauses. In one case, even the records of the processing activities, which are required to be developed by processor, cloud provider expects to be delivered by the controller.
- Art, 28, art. 35, art. 30 GDPR
- Some stakeholders provided clear answers that they do not have such documentation. One stakeholder declared that the DPIA and risk assessment were prepared but they did not provide any evidence, moreover this stakeholder was not a party to the contract based on which the GDPR documentation should be prepared according the contract, which is publicly available and was provided to us.
- It is difficult to assume what are the differences between stakeholders regarding the availability of GDPR documentation. In general, there is lack of documents with all questioned/concerned stakeholders. They are aware of a risk assessment or DPIA but as data controllers, they do not possess any.
- We are planning to stay in contact with the relevant stakeholders and based on the facts provided in questionnaire, SA would summarize the main issues and request within the set deadline to report back to SA how the move forward with the correct GDPR implementation by using cloud services.

## **3. International transfers and access by foreign public authorities**

- Only some stakeholder provided answers to questions about international transfers. Other stakeholders declared that they do not transfer personal data to third countries. Even though, from the answers provided by one of them, it is clear that there is transfer to third countries with regard to the utilisation of services mentioned. Unfortunately, we have no documentation available.
- Art. 44-46
- The stakeholders generally authorised cloud provider to transfer personal data to USA or other countries for the purpose of providing services. This general authorisation is supported by the specific appendix where additional requirements about transfers and Standard Contractual Clauses are included.
- Lack of knowledge of the stakeholders that they are using cloud service, which is transferring personal data to third countries. One of stakeholders claimed that they use cloud provider's services but in the questionnaire claimed that no personal data is transferred. Documents from one stakeholder present that Standard Contractual Clauses are signed only by cloud provider, not by data controller - stakeholder. From the documentation provided, it is not clear which version of SCC is valid (it seems that it is not the version of SCC provided in Commission implementing decision 2021/914 from 4 June 2021). In our point of view, the contractual agreement is unclear,

mainly, it is unclear what categories of data is transferred and to what locations and what are the purposes of the transfer.

- The relationships between different stakeholders are not clear, SA is not able to assess who is responsible for the relevant documentation, because the stakeholder who declared to perform transfers, referred to the general documentation where it is not the contractual party, but the documentation is concluded by another stakeholder. We interviewed this another stakeholder, who answered in his own questionnaire that no transfers are taking place. We will need to focus on the latter stakeholder and communicate about possible follow-up steps in order to achieve compliance. It seems that there are more stakeholders who are bound by these unclear clauses. SA needs to develop steps towards the stakeholders to convince them to re-negotiate the whole documentation about transfers based on the new SCC as a minimum obligation.

#### **4. Identification of roles - Controllership and sub-processors**

- Almost all stakeholders answered that they are data controllers and the cloud provider is processor. Only one stakeholder claimed that he is only user of cloud services.
- With regard to the possible use of sub-processors, they provided us with general clause from their contract about possibility to have other processor (sub-processor).
- Art. 5 (2), art. 24; 28 (2), 28 (4) and 28 (3) (d) GDPR
- In case of the concrete/specific stakeholder who is not aware of the role in terms of the GDPR, it is difficult to assess compliance with the GDPR requirements.
- With regard the engagement of other processor, two stakeholders claimed that the cloud provider does not have any sub-processor, other stakeholders pointed out to the contractual clause in their Art. 28 agreement. However, the text of the relevant clause about sub-processors in case this cloud provider is only general quotation of the relevant GDPR provisions. The Contract is stating possibility for specific or general authorisation without any possibility for data controller to object engagement of new sub-processor. As if there was just obligation to provide information from cloud provider about a new sub-processor. The scope of information that needs to be provided to data controller is not specified in the contract. Information about the consequences of disapproval to a new sub-processor is missing. On the other hand, in case of data protection rules of other cloud providers, from the documentation provided, it seems that there is prior general agreement for controller to involve sub-processor and information about new sub-processor is provided on the website of the processor (which might be continuously updated). However, the information about the engagement of sub-processor (and possibility to object by the controller) is vague – the documentation literally says that the provider provides some option to know that there is new update on the processor's website, but without any specification what some options mean and how they are implemented in practice. It seems that objection or written cancellation of the license when data controller disagrees with a new sub-processor, means termination of the affected service.
- Two stakeholders asked directly their cloud provider if there are some sub-processors engaged. Other two stakeholders simply presented the contractual clause. In general, it seems that stakeholders are not aware of any sub-processors. One stakeholder did not provide meaningful answer showing lack of any knowledge about circumstances of having another sub-processor with regard to data protection.

- In general, contract must be clear about timing of providing information and possibility to object and also provide criteria for appointing of new/another sub-processor. Interviewed stakeholders show lack of intention to consider these requirements.

##### **5. Telemetric data**

- Some stakeholders answered that they process telemetric data for the security purposes. In one case, it was difficult to assess the purpose. Two stakeholders replied that they do not process telemetric data and one replied that telemetric data is used for creation of access - based on the limited scope of personal data e.g. name, surname, telephone number, email address, job position, function or personal employment number, place of work and employer.
- 4 (1) in connection with 5 (a), 5 (b)
- In general, there is lack of knowledge about the issue. Controllers are not aware that telemetric data is personal data, they answered that telemetric data in general do not contain personal data. Consequently, there is transparency issue. Data subjects are not informed about the processing of their personal data using cloud services. From the point of view of SA and replies to the questionnaire, it is not possible to evaluate whether telemetric data is necessary and proportional for the purpose of the said processing. In case of one stakeholder, it is controversial whether telemetric data for access is actually used. Another stakeholder stated that telemetric data is not processed by cloud provider because these data is not listed in the contract with the cloud provider. However, the relevant contract specifies that other relevant data might be processed if relevant for the purpose of providing services based on that contract. Consequently SA cannot currently assess the scope of services and their purposes due to the missing documentation and lack of specification of services provided in the questionnaire.
- It seems that there are differences between stakeholders in terms of processing of telemetric data but this might be caused by the lack of knowledge about the scope of definition of telemetric data. With regard to some stakeholders, more emphasis needs to be given on the scope and purpose of telemetric data. In addition, the data is probably transferred to third countries. It seems that the same pre-formulated data protection agreement applies to all stakeholders without any limitation or assessment of responsible Stakeholder about the scope of telemetric data.
- More information about interpretation of the definition of personal data needs to be provided, although it seems difficult to set clear distinction when/at what level the telemetric data is personal data. In terms of contract, controllers should pay special attention to processing of personal data in terms of cloud services and at best to negotiate contract without processing of telemetric data if it is not necessary for the stakeholder purposes. SA will ask stakeholders to organise trainings about the cloud related topics targeting data protection obligations including telemetric data which should be provided by their Data Protection Officers and we will request them to report about this specific trainings to us.

### **Part III – Actions by the SA**

1. **Have you taken action (i.e. fact-finding exercises, informal contact, prior consultation, investigation) towards any of the stakeholders concerning the use of cloud-based services prior to launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the stakeholder, general guidance,**

**corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

- No
2. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (E.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing).**
- At this stage, we are preparing letters to each stakeholder with specific issues identified from their questionnaire. It includes request to organise special trainings led by their Data Protection Officer targeting GDPR requirements in the context of processing of personal data in clouds and sending evidence about the content of such training to SA.

#### **Part IV – Other**

1. **What is your general impression of the levels of awareness and compliance of the stakeholders you consulted concerning the use of cloud?**
- We realize that there is (very) low level of knowledge about the data protection obligations.
2. **Are there any other issues or topics that you would like to flag?**
- For those SA who faced similar situation – when each stakeholder shows lack of knowledge, what are they follow up steps? Do they consider starting with education or immediate enforcement?
3. **Are there any leading practices of the stakeholders you have contacted that you would like to share?**
- No

## 2022 Coordinated Enforcement Action

**Use of cloud-based services by the public sector**

**Adopted on 17 January 2023**

## EXECUTIVE SUMMARY

In October 2020, the European Data Protection Board (EDPB) decided to set up a Coordinated Enforcement Framework (CEF), with a view to streamlining enforcement and cooperation among Supervisory Authorities (SAs), consistently with the EDPB 2021-2023 Strategy.

In October 2021, the EDPB selected “the use of cloud in the public sector” for its 2022 Coordinated Enforcement Action.

Throughout 2022, 22 Supervisory Authorities across the EEA launched coordinated investigations into the use of cloud-based services by the public sector. The CEF was implemented at national level in one or several of the following ways: fact-finding exercise; questionnaire to identify if a formal investigation is warranted; commencement of a formal enforcement investigation, or follow-up of ongoing formal investigations.

Between November 2021 and January 2023, these SAs have discussed the aims and the means of their actions in the context of the CEF, and decided that a questionnaire would be sent to investigate public bodies. They drafted the questionnaire, then discussed the first results of their investigations, and the way they planned to bring public bodies to compliance through the CEF. Some elements, in particular the corrective measures they could decide at national level, are still under discussion.

The present joint-report aggregates the findings of all the Supervisory Authorities participating in the CEF. A particular attention is paid to 8 challenges identified by SAs during the CEF action. These include issues at the pre-contractual phase relating to the performance of a Data Protection Impact Assessment (and/or a risk assessment) and the role of the parties. With regard to the contracts with the CSP, the issues of lack of contract and difficulty to negotiate a tailored contract were identified, as well as the public bodies’ knowledge or control over sub-processors. Furthermore, challenges relating to international transfers and access by foreign public authorities are raised. Finally, processing of telemetry data and auditing are discussed.

Taking into account the possible sensitive nature and large amounts of data processed by public bodies, it is however essential that the fundamental right to the protection of personal data is guaranteed by all public administrations. The EDPB therefore underlines the need for public bodies to act in full compliance with the GDPR when using cloud-based products or services. In this regard, the report also provides a list of points of attention that stakeholders should take into account when concluding agreements with CSPs:

- Carry out a DPIA;
- Ensure that the roles of the involved parties are clearly and unequivocally determined;
- Ensure the CSP acts only on behalf of and according to the documented instructions of the public body and identify any possible processing by the CSP as a controller;
- Ensure that a meaningful way to object to new sub processors is possible;
- Ensure that the personal data are determined in relation to the purposes for which they are processed;
- Promote the DPO’s involvement;
- Cooperate with other public bodies in negotiating with the CSPs;
- Carry out a review to assess if processing is performed in accordance with the DPIA;
- Ensure that the procurement procedure already envisages all the necessary requirements to achieve compliance with the GDPR;

- Identify which transfers may take place in the context of routine services provision, and in case of processing of personal data for the CSPs' own business purposes (see related point) and ensure Chapter V provisions of the GDPR are met, also by identifying and adopting supplementary measures when necessary;
- Analyse if a legislation of a third country would apply to the CSP and would lead to the possibility to address access requests to data stored by the CSP in the EU;
- Examine closely and if necessary renegotiate the contract;
- Verify the conditions under which the public body is allowed for and can contribute to audits and ensure that they are in place.

The action undertaken by SAs in the CEF are still ongoing at national level, especially when formal investigations were launched. Accordingly, this document does not constitute a definitive statement of the actions carried out within the CEF as the purpose of this report is not to conclude on the measures to be adopted but to reflect on the actions undertaken by competent SAs and identify the possible points of attention. It may need to be updated in the course of 2023 to take into account the progress of the procedures which have not yet been completed to date and given the issues identified, further complementary work on general recommendations to public actors concerning the use of cloud service providers could be foreseen.

## Table of contents

1	INTRODUCTION.....	5
2	STATISTICS .....	7
3	CHALLENGES IDENTIFIED DURING THE CEF ACTION .....	10
3.1	Data protection impact assessment (DPIA) .....	10
3.2	Role of the parties .....	12
3.3	Negotiating tailored contracts between public bodies and cloud service providers .....	14
3.4	Sub-processors .....	15
3.5	International transfers.....	17
3.6	Risk of access by foreign governments when using non-EU CSPs storing data in the EEA...	18
3.7	Telemetry/diagnostic information.....	19
3.8	Auditing .....	20
4	ACTIONS TAKEN BY SAS .....	21
5	POINTS OF ATTENTION FOR PUBLIC BODIES.....	30
6	CONCLUSION.....	33
	Annex 1: Definitions.....	34

## 1 INTRODUCTION

In October 2020, the European Data Protection Board (EDPB) decided to set up a Coordinated Enforcement Framework (CEF)<sup>1</sup>. The CEF is a key action of the EDPB under the second pillar of its 2021-2023 Strategy<sup>2</sup>, together with the creation of a Support Pool of Experts (SPE), aiming at streamlining enforcement and cooperation among supervisory authorities (SAs).

The EDPB selected in October 2021 “the use of cloud in the public sector” for its 2022 Coordinated Enforcement Action. The reasons for this prioritisation are mainly threefold:

- (i) it is essential that the fundamental right to the protection of personal data is guaranteed by all public administrations<sup>3</sup>,
- (ii) public authorities are processing large amounts of personal (and sometimes sensitive) data, and
- (iii) the rapid development of cloud technology in all sectors is creating new risks that need to be dealt with appropriately.

The uptake of cloud services<sup>4</sup> has doubled for enterprises across the EU between 2016 and 2021 according to Eurostat<sup>5</sup>. In the public sector, the COVID-19 pandemic has intensified a digital transformation of organisations, with many public sector organisations turning to cloud services. However, in doing so, public bodies at national and EU level may face difficulties in obtaining IT products and services that comply with EU data protection rules. Because of the nature of the data processed by public administrations and the (potentially) large amount of data stored in the cloud, it is of great importance that the fundamental right to protection of personal data is properly guaranteed in all public services. All individuals (citizens as well as persons working for public services,) should be able to trust that public bodies handle their personal data with care, especially when it is processed by a third party.

Building on common preparatory work, the EDPB announced the initiation of the action on 15 February 2022. Throughout 2022, supervisory authorities across the EEA launched coordinated investigations into the use of cloud-based services by the public sector. The CEF was implemented at national level in one or several of the following ways: fact-finding exercise; questionnaire to identify if a formal investigation is warranted; commencement of a formal enforcement investigation, or follow-up of ongoing formal investigations.

Around 100 public bodies in total were addressed across the EEA, including EU institutions, covering a wide range of sectors (such as health, finance, tax, education, central buyers or providers of IT services).

---

<sup>1</sup> EDPB Document on Coordinated Enforcement Framework under Regulation 2016/679 (EDPB, 20 October 2020) <[https://edpb.europa.eu/our-work-tools/our-documents/other/edpb-document-coordinated-enforcement-framework-under-regulation\\_en](https://edpb.europa.eu/our-work-tools/our-documents/other/edpb-document-coordinated-enforcement-framework-under-regulation_en)>.

<sup>2</sup> EDPB Strategy 2021-2023, adopted on 15 December 2020.

<sup>3</sup> Letter of the Dutch Data Protection Authority to the Dutch Minister for Digitalisation on the Central Government Cloud Policy 2022, 11 November 2022, p. 1.

<sup>4</sup> By “cloud services”, we mean one or more capabilities offered via cloud computing invoked using a defined interface. By “Cloud computing” we mean a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand. (see annex 1)

<sup>5</sup> Cloud computing used by 42% of enterprises (Eurostat, 09 December 2021), <https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20211209-2>.

The present joint-report aggregates the findings of all the supervisory authorities participating in the CEF, and provides a state of play of their work. In particular, the first part of this report presents statistics on the stakeholders addressed, while the second part analyses the challenges faced by public bodies when procuring cloud services. In particular, SAs explored public bodies' challenges with GDPR<sup>6</sup>/EUDPR<sup>7</sup> compliance, as appropriate<sup>8</sup>, when using cloud-based services. These challenges related to the process and safeguards implemented when acquiring cloud services, international transfers in view of the Schrems II judgment<sup>9</sup>, and provisions governing the controller-processor relationship.

For each identified challenge, we present a short description of the issue at hand, which provisions of the GDPR apply and why this has been an issue for the participating stakeholders. In addition, we present an overview of the actions already implemented, including guidance, letters, enforcement actions or potential actions by SAs or stakeholders.

**With this first CEF action, the EDPB intends to:**

- foster GDPR-compliance of products and services, relying on cloud-based solutions, by the national and EU public sector;
- generate a deeper insight and allow targeted follow-up at EU level;
- promote leading practices through coordinated guidance and action, thereby ensuring the adequate protection of personal data.

---

<sup>6</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 (OJ L 119, 4.5.2016, p.1).

<sup>7</sup> Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

<sup>8</sup> As regards the EDPS, any references to the GDPR should be understood as corresponding references to the EUDPR.

<sup>9</sup> Facebook Ireland and Schrems (Schrems II), C-311/18, ECLI:EU:C:2020:559.

## 2 STATISTICS

The SAs decided to contact stakeholders from multiple categories. Eleven (11) SAs indicated that they have contacted a ministry of the central government (AT, BE, CZ, EDPS, EL, IT, SI, SK, EE, ES, FR), while 11 SAs have contacted independent public bodies of the central government (BE, CZ, EDPS, EL, FI, LT, SE, SK, EE, ES, PT)<sup>10</sup>. The EDPS, EL, LI, NL, FI and CY SAs have contacted buyers and vendor managers for the central government<sup>11</sup>. The PT SA has contacted a public buyer for the public health sector.

Publicly owned companies acting as processors for several public bodies have been contacted by the DE SAs, while ministries of the regional government were part of the CEF action by the BE, DE and IT SAs. An independent public body of the regional government, a buyer for the regional government and a publicly owned company acting as a processor for several regional public bodies have been contacted by the EE, IS, and IT SAs respectively. Additionally, the BE SA has contacted a publicly owned non-profit organisation that acts as an independent internal ICT service provider for public bodies. This entity acts as a processor for the public bodies and also provides a community cloud. Finally, the SI SA has contacted 3 public research institutes.

The SAs decided to contact stakeholders from multiple sectors. From the data gathered:

- the majority of SAs contacted stakeholders in the **digitalisation of the public administration/e-government sector** (BE, CZ, DE, EDPS, EL, FI, IT, SE, SK, CY, PT),
- the BE, DE, EDPS, EL, EE, ES, PT SAs decided to contact stakeholders that are active in the **health sector**,
- stakeholders in the **employment** sector were contacted by five SAs (CZ, DE, EDPS, EL, SE, and FR),
- the SE, SK, EDPS, EE, ES SAs contacted stakeholders in the **infrastructure sector**<sup>12</sup>,
- the AT, BE, EDPS, IS, SI, FR and EE SAs contacted stakeholders in the **education sector**,
- the EDPS, SE, SK, and ES SAs contacted stakeholders in the **finance sector**,
- the EDPS and the ES SA also contacted stakeholders in the **justice sector**,
- the LT SA specifically mentioned that they contacted **Statistics Lithuania**.

Additionally, the CZ SA contacted the Ministry of Interior, the DE SA contacted a stakeholder in the pension insurance sector, while the EL SA contacted a stakeholder in the immigration and asylum sector. The FR SA also investigated the Ministry of Ecological Transition, the Ministry of Culture and the Ministry for Europe and Foreign Affairs. The LI SA contacted the IT department as the buyer for the central government, the SE SA contacted three stakeholders in the social insurance sector, and the PT SA contacted a stakeholder in the social security sector. Moreover, the ES SA contacted stakeholders in the economic affairs, research, culture, and agriculture sectors and the SK SA contacted stakeholders that are active in the audit and statistics sector. Furthermore, by contacting

---

<sup>10</sup> In 2022, the EDPS has formally contacted five EU institutions, bodies, offices and agencies ('EU institutions and bodies'), which are classified, in the context of this report, as equivalent to a "ministry of the central government" or "independent public body of the central government".

<sup>11</sup> The CY SA contacted the Deputy Ministry of Research, Innovation and Digital Policy (DMRIDP), which acts as the buyer for the central government as regards to cloud services. The EDPS contacted a buyer for other EU institutions and bodies, equivalent to "a buyer for the central government". The EL SA indicated that the buyer is a ministry of the central government, the Ministry of Digital Governance. The Ministry of Digital Governance offers cloud services through the governmental Cloud (G-Cloud) to public bodies of every sector. The NL SA contacted 3 vendor managers for the central government.

<sup>12</sup> The SE SA contacted the Swedish Mapping, Cadastral and Land Registration Authority, the Swedish Civil Contingencies Agency and the Swedish Transport Administration.

processors acting for several public national and regional bodies, several sectors were involved in the actions of the IT SA such as health, finance, education.

In addition, some SAs (EDPS, DE, EL, LI, FI, and NL SAs) contacted central buyers or vendor managers that offer services to public bodies in all sectors. The SK and CY SAs indicated that the buyer they contacted offers services in the digitalisation of the public administration/e-government sector. The education sector was targeted by the buyers contacted by the IS and SI SAs, the health sector by the buyer contacted by the PT SA. The NL SA indicated it contacted vendor managers that manage the relation between the Dutch central government and the CSPs on behalf of the organisations within the Dutch central government. One of the specific tasks of most vendor managers, according to the NL SA, is to negotiate a legal/procurement framework with the CSP in order to facilitate the possible use of products and services by the organisations. Generally, the vendor managers do not buy products and services and do not commit to buy products and services as part of the legal framework, although this may happen in some cases. It is usually the decision of the government body to buy and/or commit to buy products and services from the CSP and as a consequence to use cloud services.

With regard to the number of stakeholders that the buyer provides services for, the majority of SAs responded that this information was not available to them or that the question was not applicable to them (AT, BE, CZ, DE, FI, IT, LT, NL, SE, SK, EE, ES, PT). Nevertheless, 6 SAs (EDPS, EL, IS, LI, SI, CY) specified the number of stakeholders to whom the buyer provides services. The answers provided varied, as the SI SA stated that the buyer provides services for 5 stakeholders, while the EL SA responded that the buyer provides services for approximately 150 public bodies<sup>13</sup>.

The majority of SAs (BE, CZ, DE, EE, EL, FI, IT, LI, LT, NL, SE, SI, SK, CY, ES) stated that the initial procedural framework of their action was fact finding that could in most cases serve to determine follow-up action based on the results. Some SAs also conducted or complemented existing formal investigations: the IT SA's action included new and ongoing investigations; new investigations have been launched by the AT, FR, PT and IS SAs, while there were ongoing investigations for the EDPS, and LT SAs.

The majority of the stakeholders (87 out of the 98 stakeholders that have been contacted) indicated that they use cloud service providers (CSPs) or are planning to do so by the end of 2022, reflecting the ever-increasing use of CSPs by public authorities. The majority of these stakeholders that use CSPs or are planning to do so in the near future (66 out of the 87) use cloud for internal organisation functions, including office suites, internal communication and human resources. Nevertheless, it is important to note that 48 stakeholders use CSPs for the exercise of public functions, such as services to citizens and processing of citizen's data.

Overall, in their investigations, SAs identified the involvement of the following most commonly used CSPs: Microsoft, Amazon, Citrix, IBM, OVH, Fujitsu, Oracle, Adobe, and Google. These CSPs provide the services themselves or the services are using the infrastructure of these companies.

In relation to the actions taken by stakeholders prior to or during the acquisition of a CSP, 32 out of the 87 stakeholders performed a data protection impact assessment (DPIA). Out of the 32 stakeholders that performed a DPIA, 21 specifically analysed transfers to third countries (sometimes called DTIA for Data Transfer Impact Assessment). 48 out of the 87 stakeholders contacted the DPO for advice while 41 stakeholders performed a general risk analysis. 11 out of the 87 stakeholders contacted the SA for advice.

---

<sup>13</sup> According to the EL SA, the number of 150 public bodies is taken from the publicly available information published by the central buyer at <https://www.gsis.gr/ggpsdd/orama-apostoli>.

Finally, 36 out of the 87 responding stakeholders monitor technical and organisational measures to ensure compliance. With regard to international transfers, 25 out of 87 stakeholders indicated that they have adopted technical and organisational measures, and are monitoring if changes in the regulatory landscape occur (e.g., the CJEU's judgment in the Schrems II case). Finally, only 35 out of the 86 stakeholders are conducting regular risks assessments.

### 3 CHALLENGES IDENTIFIED DURING THE CEF ACTION

This section of the report analyses some of the challenges identified during the CEF action, both by the participating SAs and/or public bodies. These include issues at the pre-contractual phase relating to the performance of a DPIA (and/or a risk assessment) and the role of the parties. With regard to the contracts with the CSP, issues of lack of contract<sup>14</sup> and difficulty to negotiate a bespoke contract were identified. Furthermore, challenges relating to international transfers and access by foreign public authorities, for example, transfer awareness and access by foreign governments also in the case of use of non-EU CSPs providing services only from the EEA, are raised. Finally, processing of telemetry data and auditing are discussed.

#### 3.1 Data protection impact assessment (DPIA)

According to Article 35 (1) of the GDPR, “where processing of personal data is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall carry out a DPIA prior to processing. A single assessment may address a set of similar processing operations that present similar high risks.”

Article 35 (3) (b) of the GDPR also provides that a DPIA shall in particular be required, in the case of processing on a large scale of special categories of data referred to in Article 9 (1), or of personal data relating to criminal convictions and offences referred to in Article 10 of the GDPR.

It can be assumed that many public sector processing operations relying on cloud services would be likely to result in a high risk to the rights and freedoms of natural persons (for instance due to processing of sensitive data or data of a highly personal nature-- like health data or personal data relating to criminal convictions and offences referred to in Article 10 of the GDPR-- and processing is on a large scale). In such cases, controllers have the obligation to perform a DPIA prior to the processing. According to the EDPB Guidelines on Data Protection Impact Assessment (DPIA), “in order to provide a more concrete set of processing operations that require a DPIA due to their inherent high risk [...] nine criteria should be considered [...]. In most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out<sup>15</sup>”. In addition, when a DPIA is not required, the appropriate technical and organisation measures should nevertheless be determined following a risk assessment, pursuant to Article 32 of the GDPR.

However, **only thirty-two out of the eighty-six stakeholders that use CSPs indicated that a DPIA has been conducted**, before the intended processing itself. The EDPB would like to reiterate that the deployment of cloud services by public bodies will often trigger a likely high risk under the GDPR. Based on the information received by SAs from public bodies, in many cases where no DPIA was not carried out, the reason for not doing so was unclear for SAs<sup>16</sup>. This could be a potential violation of the GDPR. Public bodies that have not (yet) conducted a DPIA when deploying cloud services should therefore (re)evaluate in the short term whether a DPIA should be conducted and document this evaluation.

In some cases, **stakeholders confirmed that a DPIA was performed but it was not clear whether it took any specificity of cloud services into account.**

---

<sup>14</sup> In the sense of Article 28 GDPR.

<sup>15</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 of the Art. 29 Data Protection Working Party, p.9 and 11.

<sup>16</sup> The reasons provided for not carrying out a DPIA included that the processing is carried out in the context of the use of cloud services, which do not, according to stakeholders, meet the conditions, listed either in Article 35 (3) of the GDPR or in the list established by each Supervisory Authority under Article 35(4) of the GDPR.

**Some stakeholders have also relied completely on the security measures by the CSP, or may have considered that a DPIA was neither necessary nor mandatory.** It is important to note that where cloud service providers have provided a risk assessment to the controller, this was usually an information security risk assessment. Data protection risks have generally not been sufficiently assessed in this exercise as the service provider is not aware of (i) what and how specific processing activities are taking place, (ii) the purposes of the processing and, consequently, (iii) the risks that this processing imposes on the rights and freedoms of natural persons (rather than the risks on the public body itself).

In addition, although Article 35 (1) of the GDPR provides that, when a DPIA is required, it must be carried out prior to the processing, a number of stakeholders carried out an initial DPIA only after the processing commenced.

According to Article 35 (2) of the GDPR: “**the controller shall seek the advice of the data protection officer**, where designated, when carrying out a data protection impact assessment.” However, the data protection officer (DPO) of the controller, in most cases, was not closely involved in the process. This raises concerns amongst some SAs. Close involvement of the DPO can in fact aid public bodies to implement cloud applications in a way that is compliant with the GDPR.

As stated in the Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of the GDPR, “this advice, and the decisions taken by the controller, should be documented within the DPIA.”<sup>17</sup> The DPO should also monitor the performance of the DPIA, pursuant to Article 39(1)(c) of the GDPR. Further guidance is provided in the WP29 Guidelines on Data Protection Officer 16/EN WP 243. In addition: “it is good practice to define and document other specific roles and responsibilities, depending on internal policy, processes and rules, e.g.: [...] the Chief Information Security Officer (CISO), if appointed, as well as the DPO, could suggest that the controller carries out a DPIA on a specific processing operation, and should help the stakeholders on the methodology, help to evaluate the quality of the risk assessment and whether the residual risk is acceptable, and to develop knowledge specific to the data controller context”.

According to Article 35 (11) of the GDPR, where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the DPIA at least when there is a change of the risk represented by processing operations. In this respect, a **switch to cloud services may be a change of the risk that would need to entail a review of the DPIA, and a periodic review may be needed.**

The lack of a DPIA, where necessary, may result in the inability of stakeholders to identify and effectively address the risks related to the processing of personal data in the use of cloud services. This deficiency, together with the lack of awareness suggests that stakeholders may also face difficulties fulfilling their accountability obligation to use only processors providing sufficient guarantees, according to Article 28 (1) of the GDPR (see also section 3.3).

---

<sup>17</sup> EDPB 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 of the Art. 29 Data Protection Working Party, p. 15.

### 3.2 Role of the parties

According to Article 4 (7) of the GDPR, the ‘controller’, alone or jointly with others, determines the purposes and means of the processing of personal data. “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.

Furthermore, pursuant to the accountability principle, the controller shall be responsible for, and be able to demonstrate compliance with, the principles relating to processing of personal data in Article 5 of the GDPR<sup>18</sup>. ” The accountability principle is further elaborated in Article 24 of the GDPR, 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 of the GDPR, which lays down the controller’s obligations when engaging a processor.”<sup>19</sup>

In order to fully assess the roles of the parties when using a CSP, it is important that all (subsequent) processing activities are determined. A role under the GDPR is always linked to a set of processing activities and a CSP might also, for instance, process personal data, according to Article 6 (1) (b) of the GDPR, necessary for providing the services requested by a public body. In its Guidelines on the concepts of controller and processor in the GDPR, the EDPB reminded that the Article 29 Working Party had previously stated that “the concepts of controller and processor are functional concepts: they aim to allocate responsibilities according to the actual roles of the parties. 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>20</sup>. Therefore, another key issue when procuring CSPs is the contractual allocation of the roles of controller and processor, and in particular, whether it corresponds to the factual circumstances. In most cases, the public bodies act and present themselves as controllers and the CSPs (including hyper-scalers) as processors or sub-processors. However, if there is imbalance of power between a hyper-scale CSPs and a public body, it can be difficult for the public body as a controller to negotiate the terms of the contracts in practice<sup>21</sup>.

**If the roles and responsibilities are not correctly specified, the compliance with the respective obligations of the CSP and of the public bodies under the GDPR becomes difficult.** This is because it is not clear to which extent the CSP should for example, help the public bodies to perform a DPIA, or in case data subjects exercise their rights regarding data processing in the cloud, respond to them appropriately on behalf of the public bodies. The underlying objective of attributing the role of controller is to ensure accountability and the effective and comprehensive protection of the personal data<sup>22</sup>. Clear definition of the processing activities and respective tasks allocated to CSPs are key to

---

<sup>18</sup> EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, adopted on 7 July 2021, p. 7.

<sup>19</sup> EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, adopted on 7 July 2021, p. 8.

<sup>20</sup> EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, adopted on 7 July 2021, p. 9; See also CJEU Case C-40/17 Fashion ID.

<sup>21</sup> Nevertheless, at first glance, in such situation, and as illustrated in the Guidelines on the concept of controller and processor in the GDPR, the public bodies should still be considered as a controller, given its decision to make use of a particular CSP in order to process personal data for its purposes.

<sup>22</sup> EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, adopted on 7 July 2021, p. 9.

allow the public bodies to identify and fulfil all their responsibilities arising from the GDPR for the processing for which they are controllers, including their accountability obligations, as per Article 5 (2) of the GDPR.

Furthermore, “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>23</sup>In some cases, SAs noted that the CSP may contractually envisage data processing activities for which it acts as a controller, i.e. it processes data relating to the activities of the public body for its own purposes. In particular, the role of the hyper-scalers is not always clear, especially regarding the processing of telemetry/diagnostic data that takes place for the CSPs purposes. As a result, CSPs would become independent controllers<sup>24</sup>, if they alone decide the means and purposes of this processing. When the CSP is in fact a controller for some processing operations, the onus is on them to inform data subjects, and comply with other obligations of the GDPR, e.g., accountability obligations as per Article 5 (2) of the GDPR. In addition, a legal basis for handing over of personal data by the public body and for the processing activities carried out afterwards by the CSP acting as a controller is needed. If the public body does not have such a legal basis for disclosing the personal data to the CSP, it cannot comply with the provisions of the GDPR. This can lead to situations in which a public body enables the processing of personal data from civilians and employees entrusted to the public body, by a commercial enterprise for its own purposes in violation of GDPR.

With regard to central buyers, public bodies have sometimes indicated that they considered that the central buyer has a role of processor and even in some cases, a role as an independent or joint data controller, because the central buyer has the ability to decide on the means of the processing and the selection of processors/sub-processors for providing the cloud services<sup>25</sup>. Yet, notwithstanding the complexity of the model and the difficulty to clarify the respective roles of each parties, including of the central buyers, this should not lead SAs to consider central buyers as processors or joint controllers as it is not clear, in these situations, what processing the central buyers would actually carry out.

As mentioned before, a public body processing personal data and choosing a CSP is a controller and responsible for engaging with a CSP in a GDPR-compliant way. However it is important to note that “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 SAs 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.”<sup>26</sup>

---

<sup>23</sup> EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, adopted on 7 July 2021, p. 8.

<sup>24</sup> in such a situation, CSPs and public bodies could also qualify as joint controllers together with the public bodies if they jointly determine the purposes and means of processing. In order to be permissible, this requires that an adequate legal basis and an agreement pursuant to Article 26 of the GDPR exists. This option should not be considered when the legal basis for processing by the public body is the necessity for the performance of a task carried out in the public interest by a public body.

<sup>25</sup> see p4

[https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/brief\\_over\\_inzet\\_cloud\\_service\\_providers.pdf](https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/brief_over_inzet_cloud_service_providers.pdf)

<sup>26</sup> EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, adopted on 7 July 2021, p. 8.

### 3.3 Negotiating tailored contracts between public bodies and cloud service providers

According to Article 28 (1) of the GDPR: “where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject.”

According to Article 28 (3) of the GDPR: “processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.” Article 28(3) of the GDPR lists elements that need, in particular, to be included in the contract. In practice, this means that when a public body decides to use a CSP, a bespoke contract may need to be negotiated and the terms of each processor agreement need to be tailored to the processing operation(-s), even if a standard contract is used as a template<sup>27</sup>.

In addition, according to Article 28 (10) of the GDPR: “without prejudice to Articles 82, 83 and 84, if a processor infringes the GDPR by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.”

A contract or other legal act pursuant to Article 28 (3) of the GDPR has not been established between some of the public bodies and the respective CSP, even though the processing is already ongoing. In the majority of the investigated cases, it was claimed to be difficult for the participating stakeholders to negotiate a bespoke contract, considering that CPSs generally offer standard, predetermined contracts and left no room for negotiating the terms of the contracts. The public bodies, in these cases, are often the parties with less bargaining power. Due to the imbalance of power between the parties, the participating stakeholders found themselves in situations where they could either accept the terms and conditions offered in pre-specified contracts by the CSP or decide not to use the cloud service, as there was little or no possibility to negotiate additions or amendments to it. There are however situations in which public bodies or buyers were able to negotiate bespoke contracts<sup>28</sup>. In general, public bodies in the EEA could and should, before claiming an imbalance of power, do more in using existing and often freely available information from these cases<sup>29</sup> and join forces to counter the imbalance of power.

If the public bodies cannot negotiate the terms of the contracts in practice, due to the imbalance of power, it may be difficult for them to determine the purposes and the means of the processing of personal data for the duration of the contract, and fulfil their obligations under the GDPR<sup>30</sup>. In this

---

<sup>27</sup> If a standard contract is used, the specifics of the processing on behalf of the public body will always need to be included in the contract or its annexes

<sup>28</sup> The standard contractual clauses on controller / processor can also be helpful as a guidance when drafting bespoke contracts in this type of relation. The EDPB has already issued opinions on the EU Commission SCC but also on SCC adopted by DK SA, SI SA, and LT SA. See [Opinions | European Data Protection Board \(europa.eu\)](#)

<sup>29</sup> See for instance <https://slmmicrosoftrijk.nl/downloads-dpias/>

<sup>30</sup> As stated in the Guidelines on the concepts of controller and processor in the GDPR, “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. In addition, 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”. Therefore, and as illustrated in two examples provided in these Guidelines, the public body should still

situation, where some of the purposes and means are defined by the CSP, the service provider would then be considered as an autonomous controller, according to Article 28 (10) of the GDPR and will be liable for the violation of the relevant provisions of the GDPR (e.g., lack of appropriate legal basis, information to be provided to data subjects for such processing activities, etc.). In such cases, also the public body handing over personal data to the CSP and losing control over those personal data would infringe the relevant GDPR provisions (e.g. lack of appropriate legal basis needed for providing personal data by the public body to the CSP, the information to be provided to data subjects in relation to this processing operation, etc.).

In some of the cases with a central buyer, the contract with the reseller referred explicitly to specific future agreements/contracts to fulfil the requirements of Article 28 (3) of the GDPR; however, such contracts were not presented to the SAs that conducted the CEF action.

### 3.4 Sub-processors

Article 28(1) of the GDPR provides that controllers must “*use only processors providing sufficient guarantees*” so that the processing meets the requirements of the GDPR.

According to Article 28 (2) of the GDPR, the processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall 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.

According to Article 28 (4) of the GDPR: “where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation.” Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

Based on the CEF action, it appears that, in many cases, the public bodies' knowledge or control over sub-processors involved in the processing and the extent of such processing is mainly limited to general information made available by the hyper-scalers.

In particular, most public bodies seem to have limited control over and cannot object meaningfully to the use of sub-processors or to changes of sub-processors without risking a potentially critical loss of service. When asked about sub-processors by SAs, many respondents either did not provide any information or they referred to an online list with the sub-processors of the CSPs<sup>31</sup>. In those cases, this

---

be considered as a controller, given its decision to make use of a particular cloud service provider in order to process personal data for its purposes. Insofar as the CSP does not process the personal data for its own purposes (with an appropriate legal basis under Article 6) and stores the data solely on behalf of its customers, the service provider shall be considered as a processor.

<sup>31</sup> See below, for example the lists provided by various hyperscalers.

Microsoft:[https://servicetrust.microsoft.com/ViewPage/TrustDocumentsV3?command=Download&downloadType=Document&downloadId=ede6342e-d641-4a9b-9162-7d66025003b0&tab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913&docTab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913\\_Subprocessor\\_List](https://servicetrust.microsoft.com/ViewPage/TrustDocumentsV3?command=Download&downloadType=Document&downloadId=ede6342e-d641-4a9b-9162-7d66025003b0&tab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913&docTab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913_Subprocessor_List).

is an indication that the public bodies' knowledge on sub-processors may be limited to the publicly available information by the CSP, and that public bodies do not have control over the use of sub-processors, such as knowing exactly which one is involved for what specific purposes in their particular usage of the cloud or having the chance to approve or object to a specific sub-processor.

The fact that public bodies have actually no control over the engagement of processors and sub-processors makes it difficult for them to ensure that the processing is compliant with the provisions of the GDPR, especially regarding transfers to third countries. However, it must be emphasised that this difficulty does not, in itself, exonerate the controller from its responsibilities in the processing.

Moreover, the question of whether the controller is offered a meaningful opportunity to object to changes of sub-processors was also addressed. In some cases, the public bodies had provided a general authorisation to contract sub-processors, but the controllers had no meaningful right to object, no efficient objection procedure existed (timeline, consequences etc.) and no exit strategy had been included in the processor contract<sup>32</sup>. In practice, in the cases investigated in the CEF action, several CSPs inform their customers about changes made to the sub-processors in their newsletter or on their website, but the possibility for controllers to object to the use of such processor is often limited to termination of the contract. Pursuant to Article 28 (2) of the GDPR, controllers must be offered a way to either authorise or object (in case of a general written authorisation) to the addition of replacement of other processors. The risk of not having a meaningful way to object should be assessed prior to choosing a CSP.

In addition, the contract or other legal act shall stipulate, according to Article 28 (3) of the GDPR, that the processor respects the conditions referred to in paragraphs 2 and 4 of Article 28 of the GDPR for engaging another processor. Therefore, when there is a lack of contract between the public authority and the CSP, it is a strong indication that the framework for engaging other processors is not clearly determined.

Public bodies have highlighted difficulties in negotiating different rules on the identification/changes of sub-processors since most CSPs do not seem to be inclined to change their model considering that, in many cases, the CSPs claim that, it would not be possible for them to provide services in a different way.

In this regard, differences have been identified between some of the CSPs whose services were subject to the CEF action. In one of the CSPs contracts, for example, the terms merely repeat the text of Article 28 (2) of the GDPR. Another CSPs standard contracts describes a timeline (notification period) and foresees that in case of an objection the public body and CSP will try to find a solution addressing such objection (e.g. including making the services available without the involvement of the relevant third-party sub-processor). In general, the risk of not having a meaningful way to object to a new sub-processor seems often to be underestimated, ignored or hoped to be handled when the issue arises. This can lead to a problem of a CSP using an unwanted subprocessor and a public body not being able to change CSP, and thus to non-compliance with GDPR.

---

Google: <https://workspace.google.com/terms/subprocessors.html>;

AWS: <https://aws.amazon.com/compliance/sub-processors/>

Oracle maintains lists of Oracle Affiliates and Third Party Sub-processors that may Process Personal Information available to controllers in their Support Section.

<sup>32</sup> There are rarely tools, procedures, standard data formats or services interfaces that could guarantee data, application and service portability (reversibility).

### 3.5 International transfers

In the context of the provision of cloud services, transfers may generally be envisaged in the context of routine services provision (e.g. in the cases of ‘round the clock’ services), in case of processing of personal data for the CSPs’ own business purposes (see related point) and in case of request of access to personal data by third country public authorities (see later in the text).

During the CEF action, several SAs reached out to public bodies in the EEA using hyper-scale cloud-based services, in particular software as a service (SaaS), provided by non EU-based (including US based companies). Some of these companies are based or are operating in third countries that do not offer a level of protection that was recognised as adequate according to Article 45 of the GDPR. Therefore, a public authority’s use of the software provided by the CSP, may involve transfers to many destinations that fail to ensure an essentially equivalent level of protection to the EU, including the United States of America (US). In such cases, the public body – acting as the controller – should carefully assess the transfers that may be carried out on its behalf by the CSP, e.g. by identifying the categories of personal data transferred, the purposes, the entities to which data may be transferred and the third country involved. The assessment of the international transfers of personal data taking place should be done prior to engaging with the CSP. Public bodies should provide instructions to the processor in order to identify and use a proper transfer tool and, if necessary, to identify and implement appropriate supplementary measures which ensure that the safeguards contained in the chosen transfer tool may be complied with by the importer so as to ensure that the level of protection afforded by the GDPR is not undermined when data are transferred to a third country.

When information available to the public bodies as a controller and to the supervisory authority is not sufficiently clear, it can be difficult to assess precisely what categories of data are transferred to what locations and for what purposes.

In addition, especially in the context of some SaaS implementations, it can prove impossible or extremely challenging to identify effective supplementary measures. Therefore, it would be extremely likely that the transfers would take place in breach of the transfer rules (*Schrems II* ruling), requiring the public bodies acting as controllers to identify different solutions in order to prevent or stop such transfers<sup>33</sup> e.g., by (re)negotiating contracts or using different cloud solutions which are compliant with the GDPR (e.g. compliant EEA-sovereign cloud solutions).

Finally, the results of the co-ordinated action show that in many cases, the choice of CSP was de facto made by a central buyer for the public administrations. It is therefore important to ensure that services are assessed by the central buyers in the first place so as to identify and propose to public bodies only those services which are compliant with GDPR, as this will foster compliance by design of all the public bodies using these solutions, also considering that each public body alone may not have the same negotiation power vis-à-vis the CSPs than when joining forces.

---

<sup>33</sup> See for further information on international transfers in the context of the Schrems II decision: Recommendation 1/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

### 3.6 Risk of access by foreign governments when using non-EU CSPs storing data in the EEA

The analysis of the documents received by the authorities participating in the CEF action shows that the issue of access by third country public authorities to data stored or processed within the EEA has indeed been identified by several controllers but is usually not sufficiently tackled by them, both legally and technically.

Several provisions of the GDPR require the controller/processor to ensure the protection and confidentiality of data it processes:

Firstly, **Article 28** GDPR provides for the specific obligations when processors are involved.

Indeed, Article 28(1) of the GDPR provides that the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject. Processing carried out by a processor shall also be governed by a binding contract ensuring the respect of a number of obligations such as security and confidentiality obligations taking into account among others the nature and purpose of the processing, the type of personal data, the specific tasks and responsibilities of the processor, as well as the risk to the rights and freedoms of the data subject (see Recital 81 GDPR).

Whereas Article 28(3) (a) of the GDPR provides for a possibility for processors to lawfully disregard the controllers' instructions in order to comply with legal obligations under EU/EEA laws, *e contrario* this possibility does not extend to compliance with third country legal obligations.

Indeed, such access requests by third country authorities appear to be envisaged by multiple CSPs who are part of multinational groups whereas their data processing agreements pursuant to Article 28(3) explicitly include clauses such as

*"If [CSP] receives a legally binding request for disclosure of personal information which is subject to this Policy, [CSP] will notify the controller promptly unless prohibited from doing so by a law enforcement authority and put the request on hold and notify the lead data protection authority and the appropriate data protection authority competent for the controller unless legally prohibited from doing so or where there is an imminent risk of serious harm. If [CSP] is legally prohibited from putting the request on hold, it will inform the requesting authority about its obligations under European data protection law and ask the authority to waive this prohibition. Where such prohibition cannot be waived, [CSP] will provide the competent data protection authorities with an annual report providing general information about any such requests for disclosure it may have received, to the extent legally permitted to do so"*

or

*"[CSP] will not transfer Customer Data from Customer's selected Region(s) except as necessary to provide the Services initiated by Customer, or as necessary to comply with the law or binding order of a governmental body."*

Secondly, from a legal point of view, **Article 48** provides that "any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on

an international agreement [...] in force between the requesting third country and the EU or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter”<sup>34</sup>.

Additionally, **Articles 5(1)(f), 24**, and, from a technical point of view, **Article 32 of the GDPR**, require the controller/processor to implement appropriate technical and organisational measures to ensure, in particular, the confidentiality of processing systems and services in order to mitigate the risk of unauthorised and unlawful disclosure of or access to personal data processed.

It stems from the analysis made by the authorities that the sole use of a CSP that is part of a multinational group subject to third country laws may result in the concerned third country laws also applying to data stored in the EEA. Possible requests would in this case be addressed directly to the CSP within the EEA and would concern data present in the EEA and not data already undergoing transfer. In this context, the controller/CSP would therefore not necessarily have made the assessment of this legal framework with a view to apply the relevant safeguards. The analysis of all the elements that may lead to different situations and different violations of the aforementioned relevant provisions of the GDPR in respect of the processing carried out by the processor (acting as an autonomous controller under Article 28(10) of the GDPR when it acts in violation of the instructions of the controller) and/or by the public authority itself if appropriate instructions are not provided according to Article 28(3) of the GDPR or a processor not providing appropriate safeguards as required by Article 28(1) of the GDPR is engaged.

Where the application of the legislation of the third country would lead to the possibility to address access requests to data stored by the CSP in the EEA, **a thorough analysis should therefore be made before the conclusion of the contract.**

### 3.7 Telemetry/diagnostic information

In order to provide the cloud services, CSPs process telemetry data, i.e. data relating to the use of infrastructures and services, for example, resource identifiers, tags, security and access roles, rules, usage policies, permissions, usage statistics by different kinds of users. In particular, telemetry data may for instance be used to detect, identify and respond to operational issues, such as identifying and patching bugs and fixing problems, or to measure, support, and improve the services provided. Rules are usually set forth in order to minimize human access to usage and diagnostic data and avoid the identification of individuals. Since personal data means any information relating to an identified or identifiable natural person, it is likely that many telemetry data would qualify as personal data<sup>35</sup>. From a data protection point of view, the exact role of the CSPs when processing telemetry data should be clarified. In some cases, CSPs declare that they act as controllers for the processing of telemetry data, while in other cases they consider themselves as processors on behalf of the public authorities.

Clarifying the exact role played by the CSPs when processing telemetry data is essential in order to identify the appropriate legal basis, and ensure the respect of the principles of Article 5 GDPR with particular regard to transparency, purpose limitation and data minimisation.

---

<sup>34</sup> National decisions have already been taken in some Member States. For instance, in its order of 13 October 2020, the French Council of State acknowledged the existence of a possibility of data transfer from the HDH following an access request (an information system designed to gather health data whose hosting has been entrusted to Microsoft) to the United States and requested additional safeguards, by extension to what is foreseen for transfers to protect personal data exposed to such access request when transferred to a third country.

<sup>35</sup> In addition, it must be highlighted that telemetry data may provide detailed information on users, for instance by gaining insight about the working times of employees.

**In most cases**, despite the fact that data protection risks with telemetry data were already public knowledge<sup>36</sup>, **precise information was sought from the CSPs with regard to the processing of telemetry data only because of the CEF investigation activities**. Therefore, many stakeholders seemed to lack precise knowledge about the processing of diagnostic/telemetry data by CSPs and **there** were no evaluations carried out before the start of usage, and the contract did not provide clearly and precisely what data could be collected. In this respect, compliance with Article 28 GDPR needs a careful assessment if adequate data protection clauses covering also telemetry data are not included in the contract with a CSP.

Finally, only a few of the stakeholders were aware that, in the context of the processing of cloud telemetry data, data transfers to third countries took place, and that, as a result, compliance with Chapter V of the GDPR should also be ensured.

### 3.8 Auditing

Article 28 (3) (h) of the GDPR provides that the processor shall 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.

In this respect, most stakeholders carry out periodic checks (not necessarily qualifying as audits) on the CSPs' activities through the annual verification of certification reports and the documentation made available by the CSP on their website. However, it appears that public authorities generally do not carry out specific and direct audit activities, including inspections, regarding any CSPs.

Some stakeholders indicated that generally, CSPs do not allow the performance of audits and that it is difficult to negotiate specific clauses in this regard, including obtaining access to the results of audits carried out by third parties or requesting that third parties focus their audit on specific aspects indicated by the public authority. This may lead to situations of non-compliance with Article 28(3)(h) GDPR.

---

<sup>36</sup> see <https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/techblog-telemetrie-windows-10>

## 4 ACTIONS TAKEN BY SAs

This section presents a list of decisions or other types of actions already taken at national level in the field of cloud computing by several SAs, in reverse chronological order. In particular, this section does not aim at presenting a comprehensive overview of all actions conducted by national SAs, neither does it list ongoing actions that are not finalised and on which have not yet communicated.

The FI SA has investigated the use of learning tools provided by Google as well as cookies and other trackers by ministries and other public authorities. The FI SA is also looking into the use of cloud service providers by the city of Helsinki and the use of cookies and other trackers on the websites of online pharmacies. These investigations have not yet been finalised. . In October 2022, in the context of a prior consultation, the FI SA issued a warning to the Legal Register Centre concerning e.g., risks related to transfers of personal data to third countries. In December 2022, the FI SA issued a decision regarding the use of Google Analytics web analytics service in the Helsinki metropolitan area online library, which led to information on searched books and other items ending up at Google. The practice in place also involved unlawful data transfers to the US, and in addition to Google Analytics, the controllers used Google Tag Manager on their website (in breach of Articles 44 and 46 of the GDPR). The controllers did not have a lawful basis for processing (the cookie banner did not work), and the controllers were also considered to have breached Articles 25 and 32 of the GDPR. In addition, the controllers did not provide sufficient information on the data transfers (breach of Article 13 of the GDPR). In this decision, the Deputy Data Protection Ombudsman commented on cookies and other trackers placed on websites of public authorities, and e.g. stated that people should be able to use online services of public authorities without data collection that benefits third parties. The Deputy Data Protection Ombudsman also made a point that public authorities should not use citizens' personal data as a means of payment, and a public authority should effectively assess whether a free service (such as a web analytics service) is in fact paid for with personal data. A reprimand and an order to erase the collected data (including data transferred to the US) were issued to the controllers. It should be noted that an administrative fine cannot be issued to public authorities in Finland.

On 25 November 2022, the German Data Protection Conference ('DSK') published their evaluation of Microsoft 365<sup>37</sup>. A response by Microsoft was also published<sup>38</sup>. This work follows talks with Microsoft which were initiated at the Conference meeting of 22 September 2020, where a working group led by Brandenburg and the Bavarian State Office for Data Protection Supervision (BayLDA) were requested to enter into discussions with Microsoft "to achieve timely data protection corrections and adaptations to the standards of third-country transfers for the application practice of public and non-public bodies identified by the Schrems II decision of the ECJ." In particular, the evaluation indicates that in September 2022, Microsoft updated their Data Protection Addendum ('DPA'), clarifying Microsoft's responsibility for some processing operations. However, the Conference highlights that the changes do not conclusively clarify when Microsoft acts as a processor and as a controller. Additional shortcomings were identified by the Conference.

In November 2022, the French ministry of Education answered a question from a Member of Parliament. The MP alerted the government to Microsoft's free offer of Office 365 to teachers, and in particular, to the storage of personal data on a US cloud and the extraterritoriality of US law. In his answer, the minister said that the Ministry had asked the principals to stop any deployment or extension of Office 365 as well as Google solutions, which would be contrary to the GDPR. This request

<sup>37</sup> [https://datenschutzkonferenz-online.de/media/dskb/2022\\_24\\_11\\_festlegung\\_MS365\\_zusammenfassung.pdf](https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf)

<sup>38</sup> [https://news.microsoft.com/wp-content/uploads/prod/sites/40/2022/11/DSK-Blog-Post\\_25NOV2022\\_ENG\\_FINAL.pdf](https://news.microsoft.com/wp-content/uploads/prod/sites/40/2022/11/DSK-Blog-Post_25NOV2022_ENG_FINAL.pdf)

was made in application of the circular “cloud au centre”, which invited the various ministers to ensure that the commercial cloud offers used by the public services and organisations under their authority were immune to any extra-EU regulation. The government already stated that the Microsoft 365 collaboration suite did not comply with the “cloud au centre” doctrine<sup>39</sup>.

In November 2022, following the publication of a new government-wide cloud policy in the Netherlands, the NL SA sent out two advisory letters. The SA determined in the first letter that, among others, there was insufficient mentioning of data protection risks in the cloud policy.<sup>40</sup> The second letter was aimed at all Dutch ministries and interlinked with the first letter. In this letter, the NL SA informed all ministries of their role following GDPR when choosing to use a CSP and the importance of the role of vendor managers.<sup>41</sup>

In October 2022, the EDPS issued a decision pursuant to Article 58(3) (e) EUDPR (equivalent to Article 58(3) (h) of the GDPR) conditionally authorising the use of contractual clauses for transfers of personal data between an EU institution (the Court of Justice of the EU) and a CSP (Cisco). The EDPS authorised the use of contractual clauses until 31 October 2024 given the, *inter alia*, essential function that the institution carries out in the EU, the commitment by the institution and the CSP to comply with the EUDPR and the need for a certain period of time to implement the necessary measures. However, the EDPS set a number of strict conditions to be met in order to remedy the remaining shortcomings and to ensure an essentially equivalent level of protection. This decision followed a previous EDPS decision of August 2021<sup>42</sup> authorising the use of the contractual clauses in question for 13 months.

Throughout the fall of 2022, the DK SA handled a set of related cases concerning Danish municipalities’ use of Google Workspace for Education. Originally, in September 2021, the DK SA ordered a Danish municipality to perform a data protection impact assessment in relation to their processing of personal data of the municipality’s school children by using Google Workspace for Education and Chromebooks. Upon reviewing the municipality’s documentation and assessment of the risks to the rights and freedoms of the data subjects, the SA found in July 2022 that the performed DPIA did not sufficiently address all the relevant risks of the processing activity. Consequently, the Danish DPA reprimanded the municipality for infringing a number of provisions of the GDPR, issued a ban on the use of Google Workspace for Education by the municipality, and ordered a suspension of transfer of personal data by way of Google Workspace to third countries which do not provide an essentially equivalent level of data protection. In the beginning of August 2022, the DK SA reviewed the municipalities’ renewed documentation and DPIA. Following this review, the DK SA upheld its ban on the use of Google Workspace as the assessment still did not sufficiently address the risks to the data subjects. In continuation of its decision in August, the DK SA engaged with the municipality to address and mitigate the outstanding risks, and in September 2022 the SA suspended the ban on the use of Google Workspace by the municipality conditioned on the municipality’s continued work to address and mitigate the outstanding risks together with the service provider. Under the auspices of Local Government Denmark – an organisation representing the Danish municipalities – the affected municipality along with approximately 50 municipalities which use Google Workspace in their school,

---

<sup>39</sup> cf. <https://www.legifrance.gouv.fr/download/pdf/circ?id=45205> and « Note aux secrétaires généraux des ministères; objet: doctrine “cloud au centre” et offre 365 de Microsoft » ; 15/09/2021

<sup>40</sup> <https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/ap-kabinet-moet-privacyrisico%20%99s-cloudbeleid-aanpakken>

<sup>41</sup>[https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/brief\\_over\\_inzet\\_cloud\\_service\\_providers.pdf](https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/brief_over_inzet_cloud_service_providers.pdf)

<sup>42</sup> EDPS Decision authorising temporarily the use of ad hoc contractual clauses between the Court of Justice of the EU and Cisco for transfers of personal data in the Court’s use of Cisco Webex and related services available at [https://edps.europa.eu/system/files/2021-11/17-11-2021-edps\\_decision\\_authorising\\_temporarily\\_use\\_of\\_cjeu-cisco\\_ad\\_hoc\\_clauses\\_for\\_transfers\\_cisco\\_webex\\_1.pdf](https://edps.europa.eu/system/files/2021-11/17-11-2021-edps_decision_authorising_temporarily_use_of_cjeu-cisco_ad_hoc_clauses_for_transfers_cisco_webex_1.pdf)

joined together and with the service provider to address the risks identified by the DK SA. In late November 2022, the municipalities submitted their renewed documentation following their joint effort to document their mitigation of all relevant risks and their compliant use of Google Workspace, and will submit further documentation in January 2023, for the DK SA's review.

In June 2022, the EDPS issued an opinion to an EU agency in response to a request for prior consultation on an online platform entailing the use of cloud computing services. The EDPS concluded that the specific risks related to the development and operation of the online platform had not been sufficiently identified. In particular, it recommended that the agency ensure that the contractual framework binds the processor to meet the data protection requirements and that it assess the transfers that the use of cloud services may entail.

The EDPS (as a supervisory authority) and other EU institutions and bodies (as controllers) have been closely involved in certain inter-institutional procurement procedures<sup>43</sup> relating to cloud services. This has allowed the relevant data protection (including security requirements) to be integrated already in the procurement notice and selection and were therefore reflected in the subsequent contracts. Since many data protection issues stem already from the procurement stage, such practice effectively contributes to the proper implementation of the relevant rules. The EU institutions and bodies that were already closely involved in such procedures before the Schrems II judgment have become even more involved following that judgment. In particular, this concerns greater involvement in clarifying the situations in which cloud services may be used and what safeguards and measures are already available, as well as the development of new measures additional to those already in place.

In addition, the EDPS as a controller initiated an informal consultation concerning the procurement of SaaS and hosting services from an EU-based provider. The EDPS as a supervisory authority made recommendations to the controller on data protection requirements within the procurement procedure, on the selection of providers by using relevant data protection criteria and guarantees to be required from the provider, including ensuring that processing only takes place in the EEA and that extra-territorial third-country legislation does not apply. Furthermore, the EDPS advised the controller on technical, organisational and security measures to be implemented, additional contractual clauses to be included into the model inter-institutional contract to be led by the EDPS, and on the involvement of other EU institutions and bodies. Following the procurement procedure, the SaaS will be based on Nextcloud's software and will be provided and hosted by TAS France.

In April 2022, the EDPS published a factsheet<sup>44</sup> in order to share an informal supervisory opinion issued to an EU institution that requested guidance. In the factsheet, the EDPS reminded the EU institutions and bodies of the recommendations issued following its' 2019-2020 investigation into the use of Microsoft's products and services by EU institutions and bodies as well as the EDPS' ongoing investigation into the use of Microsoft 365 by the European Commission. The EDPS also recalled the requirements and consequences of the Schrems II judgment concerning the transfers to countries outside the EEA and informed them of the 2022 Coordinated Enforcement Action.

In April 2022, the EDPS also issued a decision<sup>45</sup> to the EU agency Frontex on the latter's move to a hybrid cloud consisting of Microsoft Office 365, Amazon Web Services (AWS) and Microsoft Azure, following an investigation initiated in June 2020. The investigation looked at compliance with the

---

<sup>43</sup> Both before and after the Schrems II judgment.

<sup>44</sup> [https://edps.europa.eu/system/files/2022-04/22-04-29\\_ongoing-investigation-into-the-use-of-m365-by-euis\\_en.pdf](https://edps.europa.eu/system/files/2022-04/22-04-29_ongoing-investigation-into-the-use-of-m365-by-euis_en.pdf).

<sup>45</sup> [EDPS Decision concerning the investigation into Frontex's move to the Cloud](https://edps.europa.eu/system/files/2022-04/2022-04-12-edps-decision-frontex_en.pdf), available at [https://edps.europa.eu/system/files/2022-04/2022-04-12-edps-decision-frontex\\_en.pdf](https://edps.europa.eu/system/files/2022-04/2022-04-12-edps-decision-frontex_en.pdf)

EUDPR, taking the EDPS Guidelines on the use of cloud computing services<sup>46</sup> issued in 2018 into account. The EDPS found that the agency had moved to the cloud without a timely and exhaustive assessment of data protection risks and identification and implementation of appropriate mitigating measures. The EDPS also found that the agency had failed to observe the principles of lawfulness and data minimisation. The EDPS therefore issued a reprimand for a breach of Articles 4(2), 26 and 27 of the EUDPR<sup>47</sup> as well as an order to review and amend the DPIA and the record of processing activities to bring the processing into compliance with the EUDPR.

On 20 December 2021<sup>48</sup> and 3 May 2022<sup>49</sup>, the IS SA ordered the municipality of Reykjavík, to stop all processing of personal data of elementary-students in the Seesaw educational system<sup>50</sup>, due to several infringements of the GDPR. The processing agreement was insufficient, a specified, explicit and legitimate purpose for the processing in question was not demonstrated, and the processing was neither fair nor transparent. In addition, the principles of data minimisation and storage limitation were not implemented or data protection by design and by default, considering the amount of data collected, the extent of processing, and the period of storage. The DPIA did not meet the minimum requirements, appropriate security of the data was not demonstrated, and the data was being transferred to the US without appropriate safeguards. Finally, the infringements concerned personal data of children and it was considered likely that sensitive data were being processed.

On 23 November 2021<sup>51</sup>, the IT SA issued a favorable opinion, with some comments, on a draft Decree of the Ministry of Foreign Affairs on the testing of electronic voting in elections for the renewal of Committees of Italians Abroad. In issuing the opinion, the IT SA requested clarifications in the decree about the role carried out by the Ministry and other parties involved (e.g. CSPs) and highlighted the need to envisage the data retention period of data. Besides, the Ministry was also required to take additional measures in case of transfer of personal data in third countries to ensure a level of protection of personal data substantially equivalent to that provided for in the EU, including the encryption of personal data by the controller, with encryption keys in its exclusive availability.

On 16 September 2021<sup>52</sup>, in a decision on a complaint relating to the ‘proctoring system’ called Respondus used by an Italian University, the IT SA declared the unlawfulness of the processing carried out by the University on account of the infringement of Articles 5 (1) (a), (c) and (e), 6, 9, 13, 25, 35, 44 and 46 of the GDPR and Section 2-f of the Italian Data Protection Code and prohibited the University from further processing students’ biometric data and data on the basis of which the profiling of data subjects through the Respondus system is carried out. The Authority also prohibited the transfer of data subjects’ personal data to the US in the absence of adequate safeguards for such data subjects as a result of the absence of an appropriate and documented assessment of the relevant third country law in the light of the Schrems II ruling and issued a fine of EUR 200.000,00 (two hundred thousand).

---

<sup>46</sup> EDPS Guidelines on the use of cloud computing services by the European institutions and bodies, available at: [https://edps.europa.eu/data-protection/our-work/publications/guidelines-use-cloud-computing-services-european\\_en](https://edps.europa.eu/data-protection/our-work/publications/guidelines-use-cloud-computing-services-european_en).

<sup>47</sup> Corresponding to Articles 5 (2), 24 and 25 of the GDPR.

<sup>48</sup> <https://www.personuvernd.is/urlausnir/akvordun-um-notkun-seesaw-nemendakerfisins-i-grunnskolum-reykjavikur>.

<sup>49</sup> In addition, the IS SA decided to impose an administrative fine.

<https://www.personuvernd.is/urlausnir/notkun-seesaw-nemendakerfisins-i-grunnskolum-reykjavikur-sektarakvordun-1>.

<sup>50</sup> <https://web.seesaw.me/>

<sup>51</sup> <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9721434>

<sup>52</sup> <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9703988>. The decision is currently under judicial proceeding.

On July 23, 2021, the FR SA sent a letter to the Ministry of Health asking it to take the necessary measures to ensure the compliance of the "TOUSANTICOVID" application (which allowed users to store their Covid certificate). Indeed, during audits conducted by the FR SA, the CNIL noted that the content of the barcode was transmitted via servers located partly in the United States in order to secure the information systems used (distributed anti-denial of service device and firewall). In its letter, the FR SA asked the Ministry to consider a change of service provider in order to use a solution from a company subject to the exclusive jurisdiction of the European Union. In the meantime, the FR SA also requested that certificates to be converted be end-to-end encrypted. As of August 2, 2021, the end-to-end encryption of certificates during their transmission was effectively implemented, thus allowing the compliance of the processing. No unencrypted data relating to the evidence constituting the Covid certificate has since been transmitted to servers located outside the European Union.

In July 2021, the EDPS issued an opinion<sup>53</sup> in response to a request for prior consultation under Article 40 EUDPR<sup>54</sup> by an EU institution (the European Central Bank). In that opinion, the EDPS addressed the question whether mitigating measures identified by the institution concerned could be considered sufficient to appropriately address the high risk identified in relation to the envisaged use of the Microsoft Dynamics 365. The EDPS concluded that the envisaged measures were insufficient to mitigate those risks. As a consequence, the EDPS found that there were not sufficient guarantees and appropriate safeguards that the processing by the CSP and its sub-processors would meet the requirements of the EUDPR and ensure an essentially equivalent level of protection to that guaranteed in the EEA. The EDPS therefore issued a warning that the envisaged processing operation was likely to infringe Articles 4(2), 27, 29, 46, and 48 EUDPR<sup>55</sup>. Moreover, the EDPS made several recommendations to assist the institution in ensuring compliant processing.

In July 2021, the EDPS issued another opinion<sup>56</sup> in relation to transfers to a third country. The opinion included guidance on the use of derogations under Article 50 EUDPR<sup>57</sup> for transfers carried by a CSP for the purposes of publishing a newsletter by an EU agency. In particular, the EDPS highlighted that the agency should assess, in cooperation with the CSP, whether there were alternative newsletter publishing solutions available that do not involve the transfers of personal data to the US.

In June 2021<sup>58</sup>, as a result of an own volition enquiry, the IT SA found infringements of the GDPR arising from the configuration of the 'IO' app, a public administration app used as access point to local and national public services in Italy (among others, for example, related to tax payments, digital Covid certificates, etc.), in relation to excessive data collection and transfer to third countries, inadequate information to users, failure to request users' consent for storing information, or accessing information that is already stored, in their terminal equipment, unnecessary geolocation of users based on IP addresses. The Garante ordered to provisionally limit certain data processing activities as performed via the said app since they entailed interactions with services by Google and Mixpanel and resulted accordingly into transfers to third countries of data that are highly sensitive including information on cashback transactions and payment tools. After the publicly-owned company

<sup>53</sup> [EDPS Opinion on a prior consultation requested by the European Central Bank on their new customer relationship management system](https://edps.europa.eu/system/files/2022-04/21-07-08_edps_opinion_ecb_customer-management-system_en.pdf), available at [https://edps.europa.eu/system/files/2022-04/21-07-08\\_edps\\_opinion\\_ecb\\_customer-management-system\\_en.pdf](https://edps.europa.eu/system/files/2022-04/21-07-08_edps_opinion_ecb_customer-management-system_en.pdf)

<sup>54</sup> Corresponding to Article 36 of the GDPR,

<sup>55</sup> Corresponding to Articles 5(2), 25, 28, 44 and 46 GDPR

<sup>56</sup> [EDPS Opinion on transfers to a third country resulting from the use of a newsletter service by ENISA](https://edps.europa.eu/system/files/2021-09/21-07-27_opinion_enisa_transfers_third_countries_en.pdf), available at [https://edps.europa.eu/system/files/2021-09/21-07-27\\_opinion\\_enisa\\_transfers\\_third\\_countries\\_en.pdf](https://edps.europa.eu/system/files/2021-09/21-07-27_opinion_enisa_transfers_third_countries_en.pdf).

<sup>57</sup> Similar to Article 49 of the GDPR.

<sup>58</sup> <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9668051> and <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9670061>

managing the App committed themselves to minimize user data collected for the purpose of activating the services provided through the 'IO' app and transferred to third countries and to implement the corrective measures requested by the SA (e.g. several functions were deactivated as they allowed tracing user location via his or her IP address and unnecessary Google services were deactivated and steps were taken to prevent the contents of user alerts from being disclosed to Google), the Italian SA lifted the temporary limitation it had imposed on the processing of personal data. However, the processing will continue to be limited as for the data collected and stored by Mixpanel. Those data may not be used any longer and will only be stored by the company until the SA completes its investigations (which are still ongoing).

In May 2021, the State Data Protection Authority for the German state of Baden-Württemberg has published a press release<sup>59</sup> advising against the use of a specifically configured version of Microsoft Office 365 at schools, as part of the education platform for schools in order to provide teachers, students and parents with a suitable digital infrastructure for teaching and education, due to high privacy risks and claimed that alternative solutions should be strengthened<sup>60</sup>.

On 11 May 2021, based on a complaint, the PT SA issued a warning to a University, under Article 58(2) (a) of the GDPR on the likelihood that the data processing of its e-proctoring program infringes Article 5(1) (a) to (c) of the GDPR. The university had contracted the use of applications Respondus Lockdown Browser and Respondus Monitor as tools for monitoring examinations. Upon collection, the data was transferred to the US by AWS with no supplementary measures, pursuant to the Schrems II judgement. The PT SA also, under Article 58 (2)(d) of the GDPR, issued an order to delete data concerning staff and some students, who had already downloaded the software for training purposes before the exams, that had been transferred to the US.

In May 2021, the EDPS opened two investigations following the Schrems II judgment.<sup>61</sup> One regarding the use of cloud services provided by Amazon Web Services and Microsoft under Cloud II contracts by EU institutions and bodies, and one regarding the use of Microsoft 365 by the European Commission.

The PT SA, within an investigation into a platform set up to follow Covid-19 patients under surveillance or self-care, called 'Trace Covid19', found out that the authentication services to gain access to the platform were provided by the health establishments but synchronised with the Microsoft Azure Active Directory. The PT SA verified that the contract required by Article 28 of the GDPR was a standard contract with no possibility for inserting tailor-made clauses suitable for the data processing. The PT

---

<sup>59</sup> <https://www.baden-wuerttemberg.datenschutz.de/lfdi-raet-aufgrund-hoher-datenschutzrechtlicher-risiken-von-der-nutzung-der-geprueften-version-von-microsoft-office-365-an-schulen-ab/>.

<sup>60</sup> According to the press release, « Controllers – and these are the schools (cf. Article 4 No. 7 GDPR) – do not have complete control over the overall system and the US processor in the chosen system. According to the assessment of the State Commissioner, they are currently unable to sufficiently understand which personal data are processed, how and for what purposes, and they cannot prove that the processing is reduced to the minimum necessary for this purpose. However, they would have to do all this in order to meet their accountability under Article 5 (2) GDPR. In addition, for some transfers of personal data to Microsoft – sometimes also in regions outside the EU – no legal basis is recognizable, which is required under the GDPR. This applies in particular to international data flows in the light of the Schrems II judgment of the European Court of Justice from 2020. [...] "It does not seem completely out of the question to work legally in the school sector with other variants of the products used in the pilot test and under significantly modified operating conditions. In recent months, however, it has not been possible to find such a solution, even after intensive cooperation and a high level of human resources." (unofficial translation)

<sup>61</sup> [https://edps.europa.eu/press-publications/press-news/press-releases/2021/edps-opens-two-investigations-following-schrems\\_en](https://edps.europa.eu/press-publications/press-news/press-releases/2021/edps-opens-two-investigations-following-schrems_en).

SA made a critical assessment of the situation and provided recommendations for the controller to comply with the GDPR and to put adequate contractual clauses in place.

After the "Schrems II" ruling, the FR SA has assisted the "Conférence des grandes écoles (CGE)" and the "Conférence des présidents d'université (CPU)" in the compliance with the GDPR of collaborative digital tools used in higher education and academic research that are provided by US companies. In its press release of May 2021<sup>62</sup>, the FR SA recognized that the risk of illegal access to this data by the US authorities must be excluded. However, considering the context of the health crisis, the need for the colleges and universities concerned to ensure the continuity of operations with the use of digital tools may have justified use during a transitional period. The FR SA committed itself to provide all the necessary assistance to these colleges and universities to identify possible alternatives during that transitional period. However, the FR SA reminded that "*The European Data Protection Board has still not identified any additional measures that would ensure an adequate level of protection when a transfer is made to a cloud computing service provider*".

On 27 April 2021, following complaints, the PT SA issued an order under Article 58(2) (j) of the GDPR to suspend the data flows to the US or any other third country with no adequate protection, via Cloudflare, a company based in San Francisco, California, within 12 hours. The personal data at stake were contained in the replies provided by citizens to the National Statistics Institute. The contract between the controller and Cloudflare as processor was based on both the Privacy Shield (already invalidated by the CJEU) and SCCs with no supplementary measures adopted. The suspension was based on the Schrems II judgement.<sup>63</sup>

In the Netherlands, in the first quarter of 2021 two parties submitted a DPIA to the NL SA about the (further) use of Google G Suite/Workspace after conducting a DPIA. Firstly, the Dutch Ministry of Justice and Security submitted a request for prior consultation about the possible deployment of Google G Suite Enterprise by Dutch government organisations. Secondly, SURF and SIVON<sup>64</sup> consulted the NL SA about the (further) use of Google G Suite Education. In short, the NL SA advised against the (further) use of Google G Suite/Workspace (for education) by both parties<sup>65</sup>. This was mainly based on the high risks that were already identified in the DPIA. Among others, the outcome of the DPIA showed that there are fundamental issues relating to purpose limitation, transparency and the roles of the parties. With the advice of the NL SA, the negotiating parties reached an agreement with Google<sup>66</sup>. The Ministry has stated that all high-risks are mitigated to such an extent that they are longer classified as 'high'.

---

<sup>62</sup> CNIL calls for changes in the use of US collaborative tools by French universities, 31 May 2021, available at: <https://www.cnil.fr/en/cnil-calls-changes-use-us-collaborative-tools-french-universities>.

<sup>63</sup> Order of the PT SA, 27 April 2021, available at:

<https://www.cnpd.pt/umbraco/surface/cnlpDecision/download/121875>  
<https://www.cnpd.pt/umbraco/surface/cnlpDecision/download/121875>

<sup>64</sup> SURF is a cooperative association of Dutch education and research institutions in which the members (100+) join forces. SURF offers its members several IT services such as network connectivity, security, trust & identity, and also joint procurement of IT facilities and contract management. Sivon is also a cooperation, but with a focus on the primary and secondary educational sector. Both parties negotiate with CSPs on behalf of their members.

<sup>65</sup> Dutch Data Protection Authority on Google G Suite for Education, 08 June 2021, available at:

<https://www.rijksoverheid.nl/ministeries/ministerie-van-onderwijs-cultuur-en-wetenschap/documenten/kamerstukken/2021/06/08/advies-autoriteit-persoonsgegevens-inzake-google-g-suite-for-education>.

<sup>66</sup> Letter to Parliament on data protection agreements between Google Workspace for Education, 8 July 2021, available at: <https://www.rijksoverheid.nl/documenten/kamerstukken/2021/07/08/kamerbrief-voortgang-advisie-autoriteit-persoonsgegevens-inzake-google-g-suite-for-education>.

The NL SA also called upon the Dutch ministers for education, amongst others, to raise the issues on an EU level and start coordinated actions in order to safeguard person data in the context of cloud use for education.<sup>67</sup> In addition, SLM Rijk, which is a strategic vendor manager for public bodies in the Netherlands, had conducted several DPIAs on Microsoft and Google products on behalf of Dutch governmental organisations. The DPIAs are publicly available<sup>68</sup>.

In the context of its Schrems II Strategy,<sup>69</sup> the EDPS issued an order in October 2020, to all EU institutions and bodies to complete a transfer mapping exercise identifying which ongoing contracts, procurement procedures and other types of cooperation involve transfers of data, and to report certain results to the EDPS. The EDPS also strongly encouraged the EU institutions and bodies to avoid processing activities that involve transfers of personal data to the US. Following that order, the EDPS has received numerous requests for guidance on proper compliance, which it has provided as informal and formal supervisory opinions.

The EL SA examined ex officio the compliance of the Hellenic Ministry of Education and Religious Affairs on the compatibility of modern distance education in primary and secondary schools<sup>70</sup> -during the lockdown imposed due to the Covid-19 pandemic- with the provisions of the GDPR. In the context of the case, the updated DPA and the compliance actions of the Ministry were examined. In September 2020, the EL SA identified five deficiencies, including that no proper evaluation of data transfer to non-EU countries had been carried out, in particular in the light of the Schrems II judgement after taking into account that the processor's parent company (Cisco Inc.) is established in the USA, and that Cisco universal cloud is being used. The EL SA reprimanded the Ministry for this violation and instructed the latter to address the deficiencies<sup>71</sup> within 4 months. In 2022, the EL SA examined the Ministry's compliance with the above decision. It found that no further corrective measures were required and called on the Ministry to make the necessary amendments to improve transparency. In the decision, it is mentioned that the general issue of the application of Chapter V to videoconferencing services provided by companies – members of a group controlled by an entity subject to US law, will be examined with the other supervisory authorities through the cooperation and consistency procedures of the GDPR (Decision 61/2022<sup>72</sup>).

On April 15, 2020, the Health Data Hub<sup>73</sup>, a French public platform created in 2019 to share health data to support research projects concluded a contract with Microsoft. In an emergency procedure,

---

<sup>67</sup> [https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/brief\\_minister\\_voor\\_basis-en\\_voortgezet\\_onderwijs\\_en\\_media.pdf](https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/brief_minister_voor_basis-en_voortgezet_onderwijs_en_media.pdf)

<sup>68</sup> <https://slmmicrosoftrijk.nl/downloads-dpias/>

<sup>69</sup> [EDPS Strategy for Union institutions, offices, bodies and agencies to comply with the 'Schrems II' Ruling](https://edps.europa.eu/sites/default/files/publication/2020-10-29_edps_strategy_schremsii_en_0.pdf), available at [https://edps.europa.eu/sites/default/files/publication/2020-10-29\\_edps\\_strategy\\_schremsii\\_en\\_0.pdf](https://edps.europa.eu/sites/default/files/publication/2020-10-29_edps_strategy_schremsii_en_0.pdf)

<sup>70</sup> EL SA Opinion 4/2020 on the compatibility of modern distance education in primary and secondary schools, 7 September 2020, available at: <https://www.dpa.gr/el/enimerwtiko/prakseisArxis/gnomodotisi-se-shesi-meti-syghroni-ex-apostaseos-ekpaideysi-stis>.

<sup>71</sup> EL SA Decision 50/2021, 16 November 2021, available at:

<https://www.dpa.gr/el/enimerwtiko/prakseisArxis/diadikasia-syghronis-ex-apostaseos-ekpaideysis-apoypoyrgeio-paideias>. See in particular paragraph 20

<sup>72</sup> EL SA Decision 61/2022, 1 November 2022, available at:

<https://www.dpa.gr/el/enimerwtiko/prakseisArxis/symmorfosi-toy-ypoyrgeioy-paideias-kai-thriskeymaton-me-tin-apofasi>

<sup>73</sup> CNIL, The Health Data Hub, 9 Febarury 2021, available at: <https://www.cnil.fr/fr/la-plateforme-des-donnees-de-sante-health-data-hub>.

the Conseil d' État (High Administrative Court)<sup>74</sup> pointed out that Microsoft must refrain from transferring health data to the US. It acknowledged the risk of access by US authorities, but also that it did not justify, in the very short term, the suspension of the Hub because of the context of the health crisis and the necessity to ensure the continuity of the services offered by the Hub. The judge ordered the Health Data Hub to find a permanent solution that will eliminate any risk of access by US authorities. In accordance with the judge's request, the FR SA verified, for each request for authorization of research projects using the Health Data Hub, that the interest of the project, considering the health emergency of the Covid-19 pandemic, was sufficient to justify the risk incurred and that the use of the Hub was necessary.

In January 2020<sup>75</sup>, the IT SA issued an opinion on the draft "Guidelines — Security in ICT procurement" setting out general guidelines for public administrations when dealing with IT acquisitions as well as public service providers. Among several recommendations, the Garante highlighted the need to adequately identify, as part of the tender specifications, a correct distribution of the respective responsibilities between the controller and processors, in particular avoiding disproportionate clauses relating to liability, especially in the case of standard contracts, with almost zero trading margins on the part of the data controller.

In 2019-2020, the EDPS carried out an investigation into the use of Microsoft's products and services by EU institutions and bodies. On the basis of that investigation, the EDPS issued its Findings and Recommendations to the EU institutions and bodies.<sup>76</sup> This occurred before the Court of Justice handed down the Schrems II judgment. However, many of the identified issues anticipated that ruling. In particular, the recommendations pertained to ensuring that the EU institutions and bodies maintain proper control over the processing activities, particularly in view of the public role of the EU institutions and bodies, as well as control over what data are transferred where and how. Moreover, the EDPS recommended that the EU institutions and bodies put in place appropriate technical measures to stem the flow of personal data sent to the CSPs as well measures to be taken to ensure compliance with the transparency obligations of EU institutions and bodies towards data subjects.

Since 2019, there have been ongoing ministerial discussions in Estonia, led by the Ministry of Economic Affairs and Communications, to decide when the public sector, i.e., government and local government authorities can use cloud services. The discussions focus on workspace services (SaaS and Platform as a Service (PaaS) - e-mail, MS Office, Intranet platforms like Atlassian etc. Public sector official databases, registries are not under discussion.

---

<sup>74</sup> CNIL, The Conseil d' État asks the Health Data Hub for additional guarantees to limit the risk of transfer to the United States, 14 October 2020, available at: <https://www.cnil.fr/fr/le-conseil-detat-demande-au-health-data-hub-des-garanties-supplementaires>.

<sup>75</sup> <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9283857>

<sup>76</sup> See the [EDPS Public Paper on the Outcome of own-initiative investigation into EU institutions' use of Microsoft products and services, available at https://edps.europa.eu/sites/default/files/publication/20-07-02\\_edps\\_paper\\_euis\\_microsoft\\_contract\\_investigation\\_en.pdf](https://edps.europa.eu/sites/default/files/publication/20-07-02_edps_paper_euis_microsoft_contract_investigation_en.pdf).

## 5 POINTS OF ATTENTION FOR PUBLIC BODIES

Following the completion of the analysis of the issues identified through the CEF Action, and the review of the SAs' decisions, this section of the report provides a list of points of attention that stakeholders can take into account when concluding agreements with CSPs, without prejudice to the provisions of the GDPR.

A non-exhaustive list of possible further actions by Supervisory Authorities is also presented.

Public bodies should consider the following, without prejudice to other GDPR provisions, when using cloud services, in order to ensure that their cloud implementation complies with GDPR:

- **Carry out a DPIA**, when it is necessary for the use of cloud services, in order to determine any necessary supplementary technical and organisational measures that would be required. If the DPIA is required and was not performed prior to the processing as required by Art 35 GDPR, notwithstanding the assessment of the public body's liability, the DPIA should be performed "ex post" as soon as possible, and the technical and organisational measures identified should be implemented. **A risk assessment should at the very least be undertaken, even if a DPIA is not legally required** by the GDPR, in order to comply with Articles 24 and 32 of the GDPR. The processor should, if appropriate, provide assistance for the risk assessment, given that they may be in a better position to determine at least some of the organisational and technical measures. Only CSPs that offer sufficient guarantees should be selected.
- **Ensure that the roles of the involved parties are clearly and unequivocally determined** and precisely defined in the contract. To this end, public bodies should clearly establish their role relative to the use of cloud services, possibly through an internal assessment or within the scope of a DPIA. In addition, adequate information from the CSP and DPO consultancy are important elements so that stakeholders become aware of their responsibility and be able to distinguish and evaluate properly their roles in the processing in order to select a CSP according to the provisions of the GDPR.
- Ensure the **CSP acts only on behalf of and according to the documented instructions of the public body and identify any possible processing by the CSP as a controller**<sup>77</sup>. Public bodies should identify clearly and assess the processing operations for which the CSP intends to act as a controller in order to ensure that there is always a valid legal basis for any communications of personal data to a CSP acting as a separate (or joint) controller. Besides, the CSP will have to ensure compliance with the GDPR, including by identifying a valid legal basis in relation to the specified, explicit and legitimate purposes for which personal data are processed.
- **Ensure that a meaningful way to object to new sub-processors is possible**, for instance by proposing a meaningful right to review a change of the list of relevant sub-processors and to transmit reasoned objections within a specified period in a way that it provides a meaningful right to object. In particular, it is important to review how and when public bodies can be informed about the specific sub-processors engaged in the processing activities<sup>78</sup>, the criteria for appointing new/other sub-

---

<sup>77</sup> Although there can be situations in which a CSP is a controller, this should be an exception due to the fact that a processor should act on the documented instructions of the controller. This therefore cannot lead to a situation in which a public body who failed to do a proper risk assessment or negotiate a contract with a CSP hands over personal data from individuals to a CSP. Even in the exceptional situation in which a CSP subsequently processes personal data for a small number of purposes, the CSP will need, among others, a legal basis for the processing he is controller for. Also see art 6(4) GDPR

<sup>78</sup> Art. 28(2) GDPR provides that "The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall

processors, and under which provisions they can exercise their right to object according to Article 28(2) of the GDPR. The solutions depend on the specific circumstances of each case; however, one potential solution for a controller seeking to gain greater control over the selection of the sub-processors by hyper-scale CSPs might be to define contractually the specific criteria that any new sub-processors must meet, or to define what information the CSPs must provide on proposed new sub-processors. This could allow controllers to anticipate and mitigate risks posed to data subjects better.

- **Ensure that the personal data are sufficiently determined in relation to the purposes** for which they are processed and that they are collected for explicit and specified purposes and not further processed for incompatible purposes, including by the CSP. This could be done by way of clear and exhaustive provisions<sup>79</sup> stipulated in a **contract concluded pursuant to Article 28 (3)** of the GDPR as well as organisational and technical measures, as necessary. The controller should adequately establish its role in the processing activities and its relationship with the CSP, while the contract could specify the security controls applied by the processor and the measures to be taken in order to mitigate the risks.
- **Promote the DPO's involvement** when determining or accepting the relevant clauses. The DPO should play an active role in the analysis and negotiation of contracts offered by CSPs.
- **Cooperate with other public bodies when negotiating with the CSPs.** It is a widespread impression among the SAs and stakeholders that when various public bodies try to cooperate in negotiating with the CSPs or if one of them negotiates the same services on behalf of several public bodies, the imbalance in negotiation seems to be reduced. This is the reason why few of them already tried in the past to have talks with other entities at national level (including when possible the central buyers) at least in order to identify and discuss the main criticalities of the contracts for the services provided by the main CSPs and possible ways of addressing them. Given the hyper-scale nature of some service providers, EU/EEA countries may also consider coordinating the procurement efforts of their public authorities to compensate the imbalance.
- Carry out a **review to assess if processing is performed in accordance with the DPIA** at least when there is a change of the risk represented by processing operations (Article 35 (11) of the GDPR). A switch to cloud may be the change of the risk that would need to entail a review of DPIA, and that a periodic review may be needed. It is necessary to **regularly review and re-assess** the DPIA (and/or the risk assessment), since cloud services are dynamic and continuously subject to change.
- **Ensure that the procurement procedure already envisages all the necessary requirements** to achieve compliance with the GDPR, preferably prior to the initiation of the procurement procedure itself.
- Identify which transfers may take place in the context of routine services provision, and in case of request of access to personal data by third country public authorities. Such transfers must comply with the provisions in Chapter V of the GDPR. **Public bodies should therefore provide instructions to the CSP in order to identify and use a proper transfer tool and, if necessary, to identify and implement appropriate supplementary measures.** A renegotiation of the contract to prevent or stop such transfers, or the use of another cloud solution compliant with the GDPR, may be needed (e.g. compliant EEA-sovereign cloud solutions).

---

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.”

<sup>79</sup> The standard contractual clauses on controller / processor can also be helpful as a guidance when drafting bespoke contracts in this type of relation. The EDPB has already issued opinions on the EU Commission SCC but also on SCC adopted by DK SA, SI SA, and LT SA. See [Opinions | European Data Protection Board \(europa.eu\)](#)

**- Analyse if a legislation of a third country would apply to the CSP and would lead to the possibility to address access requests to data stored by the CSP in the EEA<sup>80</sup>.** Public bodies should therefore assess:

- 1) whether the contract provides for instructions to the CSP to process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the CSP is subject;
- 2) whether the CSP or its employees would be under the legal obligation to provide access to the data to third country public authorities and, if this is the case, would be under the legal obligation to maintain confidentiality, and would thus be prevented from informing the controller about them;
- 3) whether such access requests could be met in compliance with Article 48 (meaning with a valid legal basis and a valid ground for transfer);
- 4) whether the third country legislation provides for possible exemption/immunities for access requests concerning data processed by or on behalf of public authorities;
- 5) In particular, where no valid ways to answer the access requests would be identified, whether appropriate and proportionate technical, organisational, and/or legal safeguards according to Article 28 are in place or can be put in place<sup>81</sup>.

**- Examine closely and if necessary renegotiate the contract** with the CSP to ensure GDPR-compliance for all data processing involved, including regarding the lawfulness of processing of telemetry data.

**- Verify the conditions under which the public body is allowed for and can contribute to audits**, including inspections, conducted by the public body itself or another auditor mandated by the controller, and ensure that they are in place.

---

<sup>80</sup> It stems from the analysis led by the authorities that the sole use of a CSP that is part of a multinational group subject to third country laws may result in the concerned third country laws also applying to data stored in the EU. Possible requests might in this case be addressed directly to the CSP within the EU and would concern data present in the EU and not data already undergoing transfer. Public bodies/controllers in the EEA should therefore carry out a thorough assessment of cases where CSP in the EU/EEA could face access requests directly or indirectly from public authorities in third countries so that sufficient safeguards can be implemented. With respect to access by third country public authorities, a thorough analysis should be undertaken before the conclusion of the contract

<sup>81</sup> Similar safeguards as those provided by the EDPR in the recommendations concerning supplementary measures for transfers could be adduced.

## 6 CONCLUSION

In order to ensure a GDPR compliant implementation of cloud services, public bodies should take their responsibilities to assess and where necessary renegotiate cloud contracts, with close involvement of the DPO.

The present report is the state of play, at the end of 2022, of the CEF action regarding the use of cloud by public bodies. It may need to be updated in the course of 2023 to take into account the progress of the procedures which have not yet been completed to date and given the issues identified, further complementary work on general recommendations to public actors concerning the use of cloud service providers could be foreseen.

While this report presents a number of leading practices and points of attention for controllers using cloud services, SAs will also continue to promote compliance of cloud-based solutions, either because some of their investigations are still ongoing, or because they already envisage follow up actions.

This may include awareness raising campaigns via the publication of non-binding opinions (or recommendations) on the obligations of controllers using cloud services, on the importance of conducting a DPIA<sup>82</sup>, on the importance of signing a contract or other legal act that complies with the requirements of Article 28 (3) of the GDPR and/or on any other issues identified in this report.

Other follow-up actions may include further engaging with the public bodies/stakeholders and the CSPs concerned on the issues raised, including by setting up technical working groups, or finalising ongoing inspections, launching new investigations, and taking corrective measures where appropriate. The EDPB will also continue to raise awareness on leading practices regarding the use of cloud services.

Finally, SAs acknowledge the added-value of coordinated work under the CEF. The 2022 action has promoted a detailed and harmonised approach to GDPR compliance of products and services, relying on cloud-based solutions, by the national and EU public sector. Both the methodology and approach used for this CEF action will pave the way for more coordinated work by SAs on other topics, starting with the CEF 2023 action on the designation and role of the DPO.

---

<sup>82</sup> and on already available guidance on this matter

## ANNEX 1: DEFINITIONS

The following terminology which can be found in this document, is reused from [ISO 17788<sup>83</sup>](#)

Cloud computing	Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.
Cloud service	One or more capabilities offered via cloud computing invoked using a defined interface.
Cloud service provider	Party which makes cloud services available
Infrastructure as a Service (IaaS)	Cloud service category in which the cloud capabilities type provided to the cloud service customer is an infrastructure capabilities type.
Platform as a Service (PaaS)	Cloud service category in which the cloud capabilities type provided to the cloud service customer is a platform capabilities type.
Software as a Service (SaaS)	Cloud service category in which the cloud capabilities type provided to the cloud service customer is an application capabilities type.
reversibility	Process for cloud service customers to retrieve their cloud service customer data and application artefacts and for the CSP to delete all cloud service customer data as well as contractually specified cloud service derived data after an agreed period.
private cloud	Cloud deployment model where cloud services are used exclusively by a single cloud service customer and resources are controlled by that cloud service customer
public cloud	Cloud deployment model where cloud services are potentially available to any cloud service customer and resources are controlled by the CSP
tenant	One or more cloud service users sharing access to a set of physical and virtual resources.
hybrid cloud	Cloud deployment model using at least two different cloud deployment models
community cloud	Cloud deployment model where cloud services exclusively support and are shared by a specific collection of cloud service customers who have shared requirements and a relationship with one another, and where resources are controlled by at least one member of this collection.

---

<sup>83</sup> ISO/IEC 17788: Information technology — Cloud computing — Overview and vocabulary

## **Report of the work undertaken by the Cookie Banner Taskforce**

**Adopted on 17 January 2023**

## Table of Contents

DISCLAIMER .....	3
1. APPLICABLE LEGAL FRAMEWORK .....	4
2. APPLICATION OF THE OSS .....	4
3. TYPE A PRACTICE – “NO REJECT BUTTON ON THE FIRST LAYER” .....	4
4. TYPE B PRACTICE – “PRE-TICKED BOXES” .....	5
5. TYPE C PRACTICE.....	5
6. TYPE D & E PRACTICES : “DECEPTIVE BUTTON COLOURS” & “DECEPTIVE BUTTON CONTRAST” .....	6
7. TYPE H PRACTICE: “LEGITIMATE INTEREST CLAIMED, LIST OF PURPOSES”.....	6
8. TYPE I PRACTICE: “INACCURATELY CLASSIFIED « ESSENTIAL » COOKIES” .....	7
9. TYPE K PRACTICE: “NO WITHDRAW ICON” .....	8

## DISCLAIMER

The positions presented in this document result from the coordination of the members of the TF with a view to handling the “cookies banner” complaints received from NOYB. They reflect the common denominator agreed by the SAs in their interpretation of the applicable provisions of the ePrivacy Directive, and of the applicable provisions of the GDPR, for the analysis to be led when handling these complaints. These positions reflect a minimum threshold in this multi-layered legal framework to assess the placement/reading of cookies and subsequent processing of the data collected. They do not constitute stand-alone recommendations or findings to obtain a greenlight from a competent authority. The positions do not prejudge the analysis that will have to be made by the authorities of each complaint and each website concerned. These positions have to be combined with the application of additional national requirements stemming from the national laws transposing the ePrivacy Directive in the Member States, as well as to further clarifications and guidance provided by the national competent authorities to enforce the law transposing the ePrivacy Directive at national level, which remain fully applicable.

Following thirteen meetings of the taskforce members to coordinate their actions in handling the complaints received from NOYB, the following points were noted:

## 1. APPLICABLE LEGAL FRAMEWORK

1. Where the complaints concern the placement or reading of cookies the delegations confirmed that the applicable framework is only the national law transposing the ePrivacy Directive to the placement of cookies<sup>1</sup>.
2. Concerning the subsequent processing activities undertaken by the controller of data, meaning the processing which takes place after storing or gaining access to information stored in the terminal equipment of a user in accordance with Article 5(3) Directive 2002/58/EC (for example, the placement or reading of cookies), the delegations confirmed that the applicable framework is the GDPR (including to consent, even if given at the same moment of the placement of cookies, as far as this consent constitutes the legal basis of the subsequent processing), in line with the conclusions of EDPB Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR<sup>2</sup>.
3. In accordance with the ePrivacy framework, it was recalled that certain concepts from the GDPR (e.g. the conditions for valid consent<sup>3</sup> and the right to information) are indispensable to assess whether there is an infringement of the national law transposing the ePrivacy Directive or not.

## 2. APPLICATION OF THE OSS

4. Delegations recalled that the OSS mechanism does not apply to issues that fall under the ePrivacy Directive.
5. When the GDPR applies, the taskforce members favoured the position that article 4(23)(b) may apply but does not per se apply to complaints against website owners just because you can access the respective website from all Member States. The CSAs will be identified based on the factual elements to conclude on cross-border cases.

## 3. TYPE A PRACTICE – “NO REJECT BUTTON ON THE FIRST LAYER”<sup>4</sup>

6. It appears that some cookie banners displayed by several controllers contain a button to accept the storage of cookies and a button that allows the data subject to access further options, but without containing a button to reject the cookies.

---

<sup>1</sup> In accordance with article 15.3 of ePrivacy directive, and as it has been done in the context of these works, the EDPB shall also carry out its tasks with regard to matters covered by the ePrivacy Directive

<sup>2</sup> See also the EDPB Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications.

<sup>3</sup> By taking into consideration the EDPB Guidelines 05/2020 on consent under Regulation 2016/679

<sup>4</sup> The names of the violations used in the complaints have been kept.

7. As a preliminary remark, the task force members recalled that by default, no cookies which require consent can be set without a consent and that consent must be expressed by a positive action on the part of the user.
8. When authorities were asked whether they would consider that a banner which does not provide for accept and refuse/reject/not consent options on any layer with a consent button is an infringement of the ePrivacy Directive, a vast majority of authorities considered that the absence of refuse/reject/not consent options on any layer with a consent button of the cookie consent banner is not in line with the requirements for a valid consent and thus constitutes an infringement. Few authorities considered that they cannot retain an infringement in this case as article 5(3) of the ePrivacy Directive does not explicitly mentioned a “reject option” to the deposit of cookies.

#### 4. TYPE B PRACTICE – “PRE-TICKED BOXES”

9. It appears that several controllers provide users with several options (typically, representing each category of cookies the controller wishes to store) with pre-ticked boxes on the second layer of the cookie banner (after the user clicked on the “Settings” button of the first layer).
10. The taskforce members confirmed that pre-ticked boxes to opt-in do not lead to valid consent as referred to either in the GDPR (see in particular recital 32 “Silence, pre-ticked boxes or inactivity should not therefore constitute consent.”) or in Article 5(3) of the ePrivacy Directive.

#### 5. TYPE C PRACTICE

11. Deceptive “Link Design” It appears that some cookie banners displayed by several controllers contain a link, not a button, as an option to reject the deposit of cookies (direct link to reject or link to a second layer where a user can reject the deposit of cookies).
12. The taskforce members agreed that in any case, there should be a clear indication on what the banner is about, on the purpose of the consent being sought and on how to consent to cookies.
13. The members agreed that for the consent to be valid, the user should be able to understand what they consent to and how to do so. In order for a valid consent to be freely given, the taskforce members agreed that in any case a website owner must not design cookie banners in a way that gives users the impression that they have to give a consent to access the website content, nor that clearly pushes the user to give consent (one way could be on the contrary to allow the continuation of the navigation without cookies from the first level in particular for example).
14. The taskforce members agreed that the following examples do not lead to valid consents (non-exhaustive list):
  - the only alternative action offered (other than granting consent) consists of a link behind wording such as ‘refuse’ or ‘continue without accepting’ embedded in a paragraph of text in

- the cookie banner, in the absence of sufficient visual support to draw an average user's attention to this alternative action;
- the only alternative action offered (other than granting consent) consists of a link behind wording such as 'refuse' or 'continue without accepting' **placed outside the cookie banner** where the buttons to accept cookies are presented, in the absence of sufficient visual support to draw the users' attention to this alternative action outside the frame;

## 6. TYPE D & E PRACTICES : “DECEPTIVE BUTTON COLOURS” & “DECEPTIVE BUTTON CONTRAST”

15. It appears that the configuration of some cookie banners in terms of colours and contrasts of the buttons (“contrast ratio between the accept button and the background” – type D practice) could lead to a clear highlight of the “accept all” button over the available options.
16. The taskforce members agreed to examine type D and E practices together as the issues are linked and raise similar points of discussion.
17. The taskforce members agreed that a general banner standard concerning colour and/or contrast cannot be imposed on data controllers. In order to assess the conformity of a banner, a case-by-case verification must be carried out in order to check that the contrast and colours used are not obviously misleading for the users and do not result in an unintended and, as such, invalid consent from them. As a result, it was also agreed that a case-by-case analysis would be necessary to address specific cases, although some examples of features manifestly contrary to the ePrivacy Directive provisions have been identified.
18. Based on concrete examples, the taskforce members took the view that at least this practice could be manifestly misleading for users:
  - an alternative action is offered (other than granting consent) in the form of a button where the contrast between the text and the button background is so minimal that the text is **unreadable** to virtually any user.
19. While the design choices above are considered problematic, the taskforce members reiterated that each specific cookie banner needs to be assessed on a case-by-case basis.

## 7. TYPE H PRACTICE: “LEGITIMATE INTEREST CLAIMED, LIST OF PURPOSES”

20. It appears that some controllers put in place a banner which highlights the possibility of accepting the read/write operation at the first level (of the banner) but does not include an option to refuse at this level, which can lead the average user to believe that he has no possibility of objection to the deposit of cookies at all, and, incidentally, to the subsequent processing that results from them.

21. In addition, at the second level (of the banner), a distinction is made between the refusal given to read/write operations and the potential objection to further processing presented as falling within the legitimate interest of the data controller.
22. In those cases, it appears that:
  - The controller relied on legitimate interests under article 6(1)(f) GDPR for different processing activities as, for example, “Create a personalised content profile” or “Select personalised ads” whereas it could be considered that no overriding legitimate interest would exist for such processing activities.
  - The integration of this notion of legitimate interest for the subsequent processing “in the deeper layers of the banner” could be considered as confusing for users who might think they have to refuse twice in order not to have their personal data processed.
23. The taskforce members agreed that whether the subsequent processing based on cookies is lawful requires to determine if:
  - the storage/gaining of access to information through cookies or similar technologies is done in compliance with Article 5(3) ePrivacy directive (and the national implementing rules).
  - any subsequent processing is done in compliance with the GDPR.
24. In this regard, the taskforce members took the view that non-compliance found concerning Art. 5 (3) in the ePrivacy directive (in particular when no valid consent is obtained where required), means that the subsequent processing cannot be compliant with the GDPR<sup>5</sup>. Also, the TF members confirmed that the legal basis for the placement/reading of cookies pursuant to Article 5 (3) cannot be the legitimate interests of the controller.
25. The TF members agreed to resume discussions on this type of practice should they encounter concrete cases where further discussion would be necessary to ensure a consistent approach.

## 8. TYPE I PRACTICE: “INACCURATELY CLASSIFIED « ESSENTIAL » COOKIES”

26. It appears that some controllers classify as “essential” or “strictly necessary” cookies and processing operations which use personal data and serve purposes which would not be considered as “strictly necessary” within the meaning of Article 5(3) ePrivacy Directive or the ordinary meaning of “strictly necessary” or “essential” under the GDPR.
27. Taskforce members agreed that the assessment of cookies to determine which ones are essential raises practical difficulties, in particular due to the fact that the features of cookies change regularly, which prevents the establishment of a stable and reliable list of such essential cookies.
28. The existence of tools to establish the list of cookies used by a website has been discussed, as well as the responsibility of website owners to maintain such lists, and to provide them to the competent authorities where requested and to demonstrate the « essentiality » of the cookies listed.

---

<sup>5</sup> See EDPB guidelines on connected vehicles; also see ECJ C-597/19 para. 118.

29. On that point, it has been mentioned that specific tools exist and may be used to analyse a website and create a report that shows all the cookies that were placed when visiting the website. However, the only available tools do not allow to check the nature of the cookies but only to list the cookies placed in order to ask the website owner to provide documentation on their purposes. These tools are thus an additional help for the competent authorities to seek further clarifications and information from the website owners in addition to the information also provided on the website.
30. The [opinion n°04/2012 on Cookie Consent Exemption of WP 29](#) has also been recalled in relation to the criteria mentioned to assess which cookies are essential, and in particular the fact that cookies allowing website owners to retain the preferences expressed by users, regarding a service, should be deemed essential.

## 9. TYPE K PRACTICE: “NO WITHDRAW ICON”

31. It appears that where controllers provide an option allowing to withdraw consent, different forms of options are displayed. In particular, some controllers have not chosen to use the possibility to show a small hovering and permanently visible icon on all pages of the website that allows data subjects to return to their privacy settings, where they can withdraw their consent.
32. Website owners should put in place easily accessible solutions allowing users to withdraw their consent at any time, such as an icon (small hovering and permanently visible icon) or a link placed on a visible and standardized place.
33. The ePrivacy Directive’s reference to consent in the GDPR includes both a reference to the definition of consent (article 4 of the GDPR) as well as to the conditions of it (article 7 of the GDPR).
34. In addition to the requirements for the collection of consent to be valid in accordance with the GDPR and under Article 5(3) ePrivacy Directive, three additional cumulative conditions are mandatory (i) the possibility to withdraw consent, (ii) the ability to withdraw consent at any time, (iii) withdrawal of consent must be as easy as to give consent.
35. However, website owners can only be imposed that easily accessible solutions are implemented and displayed once consent has been collected, but they cannot be imposed a specific withdrawal solution, and in particular to set up a hovering solution for the withdrawal of consent to the deposit of cookies and other trackers. A case-by-case analysis of the solution displayed to withdraw consent will always be necessary. In this analysis, it must be examined whether, as a result, the legal requirement that it is as easy to withdraw as to give consent is fulfilled.

## **Report of the work undertaken by the supervisory authorities within the 101 Task Force**

**28 March 2023**

## Table of contents

DISCLAIMER.....	3
1 Background .....	4
2 Assessment.....	4
2.1 Transfers of personal data.....	4
2.2 Principle of accountability .....	5
2.3 Allocation of roles.....	5
3 Outcome of the complaints.....	6

## DISCLAIMER

The EDPB created the 101 Task Force to promote cooperation and effective exchange of information between the Supervisory Authorities on this specific subject-matter, in accordance with Article 70(1)(u) GDPR. The positions presented in this document result from the coordination of the Supervisory Authorities taking part in the task force with a view to handling the “101 complaints” received from NOYB regarding the tools “Google Analytics” and “Facebook Business Tools”. They reflect the common denominator agreed by the Supervisory Authorities in their interpretation of the applicable provisions of the GDPR. The positions do not prejudge the analysis that will have to be made by the Supervisory Authorities of each complaint and each tool concerned. In particular, it must be taken into account that the circumstances may change over time, for example, in case the aforementioned tools change from a technical point of view or in case the legal framework changes. The positions of the Supervisory Authorities expressed in this report do not represent the position of the EDPB.

## 1 BACKGROUND

1. On 17 August 2020, a total of 101 complaints were lodged with the European Supervisory Authorities (hereinafter: "SAs") by NOYB regarding transfers of personal data to the USA. The complaints revolve around the implementation of the tools "Google Analytics" and "Facebook Business Tools" (hereinafter: "tools") on a website and the subsequent processing<sup>1</sup> of personal data that may follow because of such implementation.
2. During the Plenary meeting of the European Data Protection Board (EDPB) on 2 September 2020, it was decided that a task force shall be established in order to ensure a consistent approach to handle the complaints ("101 task force", SAs participating in the "101 task force" are hereinafter referred to as "TF members").
3. The TF members focused their analysis on the subsequent processing that should comply with the requirements of the GDPR and that may be subject to cooperation. Following several meetings of the TF members to coordinate their actions, the following points were noted:

## 2 ASSESSMENT

### 2.1 Transfers of personal data

4. In general, before assessing the lawfulness of transfers of personal data within the meaning of Chapter V of the GDPR, controllers must ensure that all other provisions of the Regulation are complied with<sup>2</sup>. For example, if a certain tool is being used for collection of personal data on a website without a legal basis within the meaning of Article 6(1) GDPR, the data processing is unlawful, even if there were no issues with the requirements of Chapter V GDPR.
5. However, due to the subject matter of the present complaints, the following assessment will be limited to issues related to Chapter V of the GDPR.
6. The TF members agreed that there was no compliance with Chapter V of the GDPR if the transfer was based on the invalidated EU-US adequacy decision after 16 July 2020<sup>3</sup>. Furthermore, there was an agreement that concluding standard data protection clauses pursuant to Article 46 (2)(c) GDPR with retroactive effect, as brought forward by an entity in a complaint case, is not permissible<sup>4</sup>.
7. Where standard data protection clauses were concluded, and supplementary measures implemented as appropriate safeguards, the TF members recall that such measures must address the specific deficiencies identified by the ECJ in its judgement from 16 July 2020<sup>5</sup> in the assessment of the situation in the third country<sup>6</sup> in order to ensure that this legislation will not impinge on the safeguards adduced.

---

<sup>1</sup> The term "subsequent processing" refers to the processing operations which take place after storing or gaining access to information stored in the terminal equipment of a user in accordance with Article 5(3) Directive 2002/58/EC (for example, the placement or reading of cookies).

<sup>2</sup> EDPB Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, version 2.0, paragraph 5.

<sup>3</sup> ECJ C-311/18 (Schrems II), paragraph 201.

<sup>4</sup> According to the wording of Article 44 and Article 46 (1) GDPR, the appropriate safeguards must be in place before the transfer of personal data.

<sup>5</sup> ECJ C-311/18 (Schrems II).

<sup>6</sup> EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, paragraph 75.

8. In this context, the TF members agreed that encryption by the data importer was not a suitable measure if the data importer, as provider of the tool, has legal obligations to provide the cryptographic keys<sup>7</sup>. In addition, there was an agreement that anonymization functions, such as the anonymization of the IP address, are not a suitable measure where the anonymization takes place only after all the data has been transferred to the third country to the importer<sup>8</sup>.
9. Furthermore, in cases where a processor acts as data exporter on behalf of the controller (the website operator), the controller is also responsible and could be liable under Chapter V of the GDPR, and also has to ensure that the processor provides for sufficient guarantees under Article 28 GDPR<sup>9</sup>.

## 2.2 Principle of accountability

10. In cases where website operators are regarded as controller, they must carefully examine whether the respective tool can be used in compliance with data protection requirements<sup>10</sup>. The European Court of Justice (ECJ) interprets the accountability principle as requiring every data controller to be able to demonstrate that appropriate measures have been taken to safeguard the right to data protection, in order to prevent any breaches of the provisions of the GDPR.<sup>11</sup>
11. If such evidence cannot be provided (and tools are integrated on a website without a prior compliance check), in particular in case of joint-controllership, this may result in a breach of the principle of accountability. Following a case by case analysis, in particular where the controller is not in a position to provide sufficient elements to demonstrate how transfers take place, this could lead to a breach of Article 5(2) and Article 24(1) GDPR in accordance with the accountability principle stipulated in these Articles.
12. The TF members emphasise that not only the website operators (as controllers), but also the respective provider of tools who process personal data must ensure continuous compliance with the GDPR, either because the provider of the tool is, at least concerning certain processing operations, regarded as controller or, where the provider is qualified as a processor, due to the assistance obligations specified in Article 28 GDPR.

## 2.3 Allocation of roles

13. As the decision of a website operator to integrate and use third-party tools (such as social media plugins or analytics tools,) regularly results in the processing of personal data of the website visitors, this could entail liability for the website operator, even if the liability may be limited to certain processing operations<sup>12</sup>.
14. In the context of the present cases, the TF members agreed that the decision of a website operator to use a specific tool for specific purposes (for example, analyzing the behavior of the website visitor) is

---

<sup>7</sup> EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, paragraph 81.

<sup>8</sup> As it cannot be ruled out that access to the data will take place between the transfer to the third country and anonymization.

<sup>9</sup> EDPB Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, version 2.0, paragraph 19.

<sup>10</sup> In addition, the requirements of Article 5(3) of Directive 2002/58/EC (ePrivacy Directive) may be applicable. This is the case when information is stored or accessed to in the terminal equipment of a user (for example, the placement or reading of cookies). For more information, the EDPB recommends its Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR as well as its Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications.

<sup>11</sup> ECJ C-129/21 (Proximus), paragraph 81.

<sup>12</sup> ECJ C-40/17 (Fashion ID), paragraph 74.

regarded as determining the “purposes and means” pursuant to Article 4(7) GDPR. Save for those cases in which the SA’s analysis provides otherwise, those website operators are hence to be regarded as controllers for the processing of personal data of the website visitors that takes place within the context of the use of the tools on those websites. The degree of liability for the processing operations, however, must be determined on the basis of a case-by-case analysis, taking into account the different functions and options the respective tool provides.

15. Concerning such case-by-case analysis, the TF members recall that the allocation of roles is the result of a thorough analysis of objective factors, including the factual elements or circumstances of the case<sup>13</sup>. In particular, the conclusion of agreements pursuant to Article 28 or Article 26 GDPR between website operators and providers does not limit the assessment and qualification retained by SAs.

### 3 OUTCOME OF THE COMPLAINTS

16. This common assessment has enabled several SAs to adopt consistent decisions in the present “101 complaints”<sup>14</sup>.
17. Notably, SAs have ordered website operators to comply with the requirements of Chapter V of the GDPR, and if necessary, to stop the transfer at stake. Part of these decisions have been adopted in the framework of the One-Stop-Shop mechanism, in cooperation with all concerned SAs. In some cases, website operators have stopped using the tools at stake before any decisions by the SAs, which, in practice, resulted in decisions without any suspension order.
18. Furthermore, additional guidance and practical recommendations have been provided by Several Authorities to follow up on the consequences of these decisions with regards to alternative solutions.
19. Further decisions are expected in due time regarding the remaining complaints for which decisions have not been adopted yet.

---

<sup>13</sup> EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, version 2.1, cf. paragraph 12.

<sup>14</sup> At this point of time, the following SAs have already issued decisions in the context of the present complaints: AT, DK, EE, ES, FI, FR, HU, IT. Furthermore, the TF members note that the EDPS has also issued a decision in relation to “Google Analytics” in the complaint case 2020-1013 against the European Parliament.

# EDPB Documents



## Template Acknowledgement of Receipt

Adopted on 20 June 2023

Date of submission: .....

Reference number [*If available*]: .....

We acknowledge receipt of your complaint with the XX SA, [also attached for your record].

A preliminary assessment of your complaint will be conducted to determine its admissibility.

If your complaint is deemed inadmissible, you will be informed of the reasons for such decision [*SAs can specify the ground for inadmissibility, if required by their national law/practice*]. If your complaint is admissible, we may, if necessary, request additional information prior to initiating the investigation procedure.

The XX supervisory authority will inform you on the progress and the outcome of the complaint handling, including the possibility of a judicial remedy, in accordance with Article 77(2) GDPR.

Please bear in mind that the XX SA receives a high number of requests and that we are doing our best to process your complaint as quickly as possible. Please also be informed that if your complaint is subject to the cooperation procedure under Article 60 of Regulation 2016/679 [[link to additional information on the SA's website](#)], more than one European supervisory authority will be involved in handling your complaint.

Under Article 78 GDPR, without prejudice to any other administrative or non-judicial remedy, you shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning you.

If you do not receive information on the progress or outcome of your complaint within 3 months [or applicable deadline depending on the SA], you can request an update on its status by contacting us via [...] and mentioning the date of submissions/ your name / reference number indicated above [*SAs can chose depending on their practice*].

# EDPB Documents



## Template Complaint Form

Adopted on 20 June 2023

## 1. Introduction

Before lodging a complaint, please read more about your right to lodge a complaint [*link to page with additional information on the SA's website*], as well as our privacy notice [*link to SA's privacy notice*], in order to be informed about how we will process your data during this procedure.

[*Optional - Add reference here, as appropriate, to limitations under national law - e.g. if complaints are not admissible before your SA unless the SA is competent for the place where the complainant works or is resident, or where the infringement occurred*].

[*Optional - Reason to submit your complaint to this specific authority (please select the options that apply to you)*:

- a) It is the data protection authority of my place of residence;
- b) It is the data protection authority of my place of work;
- c) It is the data protection authority of the place where the alleged infringement happened;
- d) It is the data protection authority which is competent to the data protection supervision of the data controller.

Please note that your complaint might be subject to the cooperation procedure (also known as the “One-Stop-Shop” procedure, or “OSS”), if it concerns personal data processing that takes place in multiple EU/EEA countries or affects data subjects in more than one EU/EEA country. In that case, more than one European supervisory authority will be involved in handling your complaint. You can learn more about the “One-Stop-Shop” procedure through the [European Data Protection Board website](#), in particular through this [link](#) [and through this link \*\*\*[link to national page in the national language](#)\*\*\*]

## 2. Scope of the complaint form

This form is only applicable to complaints concerning possible infringements in connection with the processing of your personal data in accordance with Article 77 GDPR and [add reference to national legislation as appropriate]. Please note that this form should not be used for drawing the supervisory authorities’ attention to specific alleged infringements of data protection legislation, which do not concern you directly as a data subject.

For general inquiries and information, in particular on how to exercise your data subject rights vis-à-vis the controller, please contact us through the following [[link](#)].

[*SAs with specific templates for specific types of complaints or sectors of activities (e.g. revenge porn, internet or bank sector), can add here a reference to them, e.g. for complaints concerning “revenge porn”/ “data breaches”, please use the following specific template*]

You can submit your complaint via this electronic form. Alternatively, you may also download it, fill it in and send it to the XX authority [indicate address].

Please note that the use of this form is not mandatory for the submission of your complaint, but is intended to facilitate your submission, its completeness, and the procedure to handle it.

### **3. Complaint**

#### **3.1. Person filling the complaint**

- You personally, as concerned data subject
- Legal representative acting on behalf of (a) concerned data subject(s) / Body, organisation or association acting on behalf of (a) concerned data subject(s) [*if this option is chosen, please also specify the concerned data subject(s)' details below*]
- Body, organisation or association acting on its own initiative [*if this option is chosen, you may also specify the concerned data subject(s)' details below, where relevant*]

#### **3.2. Contact details**

##### **3.2.1. Data subject(s)' contact details [each SA can indicate whether any of these fields is mandatory according to national administrative law / provisions]**

- a) Full name and surname;
- b) Postal address, city, country;
- c) Email address - if preferred means of contact, please tick the box;
- d) Telephone / mobile number - if preferred means of contact, please tick the box;
- e) Identification details [*depends on each SA - can be personal identification number, ID / passport number or copy*].

##### **3.2.2. Contact details of the legal representative acting on behalf of the data subject(s) / Body, organisation or association acting on behalf of the data subjects(s) or on its own initiative <sup>1</sup>**

- a) Name / surname of individual / entity;
- b) Postal address, city, country;
- c) Email address;
- d) Telephone / mobile number.

#### **3.3. Subject of your complaint**

##### **3.3.1. Your complaint**

Please provide the reasons for your complaint in as much detail as possible, describing the facts in chronological order. If possible, please also clarify what is the alleged infringement of the GDPR and what is the remedy/action that you seek (e.g. rectification of your personal data; erasure of your personal data; etc.).

---

<sup>1</sup> Please provide the relevant documentation under Section 3.3.3 of this form.

3.3.2. Entity / individual which is the subject of your complaint (e.g. company, association, public authority, natural person) [each SA can indicate whether any of these fields is mandatory according to national administrative law / provisions]

- a) Name;
- b) Postal address, city, country;
- c) Contact details, i.e. telephone number, email address and website link;
- d) Company registration number
- e) Indication of whether you contacted this entity/its Data Protection Officer/individual prior to submitting your complaint:
  - If [Y], please provide all exchanges, including any replies, in attachment to this submission under section 3.3.3 below;
  - If [N], please indicate why not [for SAs which have such contact as a requirement, it can be handled here]

3.3.3. Attachments/materials provided to support your claims [each SA to determine which ones are mandatory according to national provisions]:

- a) Copy of all relevant past correspondence with the entity/individual subject of the complaint (e.g. copy of the request for the exercised right(s) and documentation proving the date the entity became aware of the request; when the request was made via email, a copy of the message sent to the entity showing the date and email addresses of sender and recipient; exhaustion of a deadline)
- b) Copy of any marketing messages or e-mails
- c) Pictures, screenshots
- d) Expert reports
- e) Witness reports
- f) Identification of the processing activities
- g) Inspection reports
- h) For legal representatives, document(s) demonstrating your capacity to file this complaint (e.g. power of attorney, mandate, notarial deed, court/private document identifying both grantor and representative, chamber's id number, address and contact data)
- i) Other (please specify)

#### 4. Acknowledgements and signature

I understand that the XX SA may, for the purpose of the examination of my complaint, be required to transfer the information collected through this form to the data controller against whom the complaint is made, and/or to another SA if necessary for the cooperation

*mechanism. The XX SA will only transfer such information if it is necessary for the handling of the complaint. In specific situations [the SA can specify, if required by national law/practice], the XX SA will maintain my anonymity.*

*[Optional] I declare, [under civil and criminal liability], that the data provided by this complaint are true and no information has been omitted or misrepresented.*

*[Signature of complainant / legal representative] [SAs can choose to have a specific authentication method when implementing this template]*

Date and place:

## Decision of the European Data Protection Board on Records management

Adopted on 20 September 2023

## Table of contents

1	Purpose .....	4
2	Definitions .....	4
3	Scope .....	6
4	Roles and responsibilities .....	6
4.1	The EDPB, represented by its Chair .....	6
4.2	EDPB Chair and Deputy Chairs.....	7
4.3	All EDPB staff.....	7
4.4	EDPB members' representatives and staff.....	7
4.5	Records manager .....	7
4.6	Document management officer.....	8
5	Principles governing Records Management.....	8
5.1	Records management systems.....	8
5.2	Capture and filing of records .....	8
5.3	Storage and Preservation .....	9
5.4	Retention, transfer and elimination .....	9
5.5	Access to records .....	10
5.6	Records Management and Personal Data.....	10
5.7	Information security .....	10

## The European Data Protection Board

Having regard to Regulation (EU) No 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 (General Data Protection Regulation)<sup>1</sup>,

Having regard to Regulation (EU) No 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data<sup>2</sup>, (hereinafter Reg. 2018/1725)

Having regard to Regulation (EEC, EURATOM) No 354/83 concerning the opening to the public of the historical archives of the European Economic Community and the European Atomic Energy Community, and amended by Council Regulation (EC, EURATOM) No 1700/2003 and Council Regulation (EU) 2015/496 of 17 March 2015<sup>3</sup>,

Having regard to Regulation (EC) No 1049/2001 regarding public access to European Parliament, Council and Commission documents<sup>4</sup>,

Having regard to Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union<sup>5</sup>,

Having regard to Article 24 of ‘The European Code of Good Administrative Behaviour’<sup>6</sup>,

Whereas:

(1) The European Data Protection Board, as a European body, is subject to legal requirements for implementing and keeping adequate records of its functions and activities and confirms its commitment to capturing and managing records with appropriate evidential characteristics in accordance with the requirements of this legal and regulatory framework.

(2) The European Data Protection Board acknowledges that uniform record-keeping practices are fundamental to ensure transparency and good administrative behaviour; enhance business continuity; and facilitate access to knowledge.

(3) All European Data Protection Board records shall be systematically and efficiently managed throughout their entire lifecycle, i.e. from their capture up to their destruction or permanent archiving. With this aim in mind, the European Data Protection Board has made an agreement with the European Commission for the use of their HAN (Hermes, Ares, NomCom) document management system. The European Commission acts as a data processor in accordance with Article 3 Reg. 2018/1725, under instructions from the EDPB, which acts as the controller of personal data in its records.

(4) Selected records shall be deposited in the historical archives at the Historical Archives of the European Union at the European University Institute (EUI) in Florence (hereafter ‘European Union’s historical archives’). The EUI acts as a data processor in accordance with Article 3 Reg. 2018/1725,

---

<sup>1</sup> OJ L 119, 4.5.2016, p. 1–88.

<sup>2</sup> OJ L 295, 21.11.2018, p. 39.

<sup>3</sup> OJ L 043, 15.2.1983, p.1

<sup>4</sup> OJ L 145, 31.5.2001, p. 43–48.

<sup>5</sup> OJ L 193, 30.7.2018, p. 1–222.

<sup>6</sup> Approved by European Parliament resolution of 6 September 2001.

under instructions from the EDPB, which acts as the controller of personal data contained in its historical archives, deposited at the EUI.

(5) This decision aims to provide the basis for consistent, sustainable and efficient records management by defining the method for the management of both paper and electronic records as a source of evidence and information. The decision may be complemented by implementing rules on specific topics.

**HAS DECIDED THE FOLLOWING:**

## 1 PURPOSE

1. The EDPB is a body of the European Union with legal personality (Article 68.1 GDPR), composed of its members (Article 68.3 GDPR). The EDPB is supported by the EDPB Secretariat, which is provided to the EDPB by the EDPS (Article 75.1 GDPR). A Memorandum of understanding, signed by the EDPB and the EDPS, defines the relationship between both bodies in relation to the EDPB Secretariat<sup>7</sup>. Managing the records of the EDPB is one of the functions fulfilled by the EDPB Secretariat. The records of the EDPB Secretariat, attesting to the fulfilment of its tasks, are inextricably linked with the records of the EDPB.

## 2 DEFINITIONS

2. For the purpose of this decision, the following definitions shall apply:
  - (1) ‘European Data Protection Board’ (hereinafter referred to as ‘EDPB’ or the ‘Board’) shall mean the body defined in Articles 68 to 76 of Regulation 2016/679 (hereinafter referred to as the ‘GDPR’) and include its Secretariat; Where this decision refers to the EDPB, this shall include the EDPB Secretariat;
  - (2) ‘EDPB members’ shall mean members of the EEA data protection authorities that compose the Board, and the European Data Protection Supervisor;
  - (3) ‘EDPB staff’ shall mean staff of the Secretariat responsible, on behalf of the EDPB and its Secretariat, for the performance of the activities of the Board that involve records management;
  - (4) ‘EDPB members’ representatives and staff’ shall mean individuals appointed or employed by EDPB members who participate in activities of the Board on behalf of that member.
  - (5) ‘Author’ shall mean the individual, group or organisation which produces a record.
  - (6) ‘Authenticity’ shall mean that a record must be what it claims to be.
  - (7) ‘Capture’ shall mean the insertion of a document into an official electronic repository by combining a unique identifier and metadata.
  - (8) ‘(Case) file’ shall mean an aggregation of records organised in line with the EDPB’s activities, for reasons of proof, justification or information and to guarantee efficiency in the work; the group of records making up the file is organised in such a way as to form a coherent and relevant unit in terms of the activities conducted by the EDPB, including its Secretariat.

---

<sup>7</sup> In light of Article 75 GDPR and the memorandum of understanding between the EDPS and the EDPB signed on 25 May 2018 ([https://edpb.europa.eu/our-work-tools/our-documents/memorandum-understanding/memorandum-understanding\\_en](https://edpb.europa.eu/our-work-tools/our-documents/memorandum-understanding/memorandum-understanding_en)), files related to financial management and human resources are managed by the EDPS. Records belonging in these files are excluded from the scope of this Decision. EDPB staff is obliged to assist the EDPS with their obligation to capture records on these matters.

(9) ‘Context’ shall mean the organisational, functional, and operational circumstances surrounding record’s creation, receipt, storage, or use, and its relationship to other records.

(10) ‘Filing plan’ shall mean the logical and hierarchical organisation of files into a tree of topics based on an analysis of the business functions and activities of the EDPB. It provides a common and standard framework enabling files to be intellectually organised and linked to the context in which they were drawn up, on the basis of the functions, activities and working processes.

(11) ‘(Historical) archives’ shall mean:

- a. Those records that are appraised as having continuing value. Traditionally the term has been used to describe records no longer required for current use, which have been selected for permanent preservation. Also referred to as permanent records.
- b. An organisation (or part of an organisation) responsible for appraising, acquiring, preserving and making available archival material.

(12) ‘Integrity’ shall mean a record must be complete and unaltered.

(13) ‘Metadata’ shall mean any information describing the context, content and structure of records and their management over time for the purposes of, inter alia, retrieval, accessibility and reuse.

(14) ‘Preservation’ shall mean processes and operations involved in ensuring the technical and intellectual survival of authentic records through time.

(15) ‘Record’ shall mean any structured information created or received by the EDPB and set aside by means of registration, protected against intentional or accidental alterations and retained as evidence and information of EDPB/EDPB Secretariat activities in pursuance of institutional and legal obligations or in the transaction of its business. Where this decision refers to EDPB records, it should be understood to also refer to EDPB Secretariat records.

(16) ‘Reliability’ shall mean that a record must be a full and accurate representation of the business transactions, activities, or facts to which it attests.

(17) ‘Registration’ shall mean capturing a record into a register, establishing that it is complete and properly constituted from an administrative and/or legal standpoint.

(18) ‘Retention list’ shall mean a description of the administrative retention period for records as well as the action to be taken following its expiry. The administrative retention period sets out the minimum period for retaining records and files - in the custody of the EDPB - according to their legal, business and accountability requirements. After the lapse of specified retention periods, the document authorises, on a continuing basis, the destruction of those records and files identified as having no further (archival) value. Further, this document identifies records that shall be transferred to the historical archives, either in their entirety or following a further assessment. The retention plan is based on the assessment of the business, legal administrative, financial and historical value of records and files.

3. For the purpose of this decision, the terms ‘personal data’, ‘controller’ and ‘processor’ shall be understood within the meaning of Article 3 of Reg. 2018/1725.
4. For the purpose of this decision, the term ‘document’ shall be understood in the meaning of Regulation (EC) 1049/2001 of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

### 3 SCOPE

5. This decision applies to EDPB records, irrespective of their form, medium (e.g. written on paper or stored in electronic form or as a sound, visual or audiovisual recording), age and location. EDPB records may arise from EDPB related activities undertaken by the EDPB Chair, the EDPB Deputy Chairs, the EDPB members' representatives and staff as well as EDPB staff in their professional capacity. EDPB records may be created or received through EDPB or non EDPB devices, or through online communication tools, including social media.
6. This decision covers drafts insofar as they are of significant long-term value, of academic interest, necessary to protect essential interests of the EDPB or the European Union, or if the content of the draft in question is likely to be of significant use to the EDPB's future work. Drafts with consolidated input which are circulated to EDPB Members for discussion in EDPB plenary meetings or expert subgroup meetings, are in principle considered as EDPB records covered by this decision. Other drafts are presumed not to fulfil the aforementioned criteria and thus not covered by this decision, unless decided otherwise by the records manager.
7. Not covered by this decision are
  - documents used and kept for reference and information only;
  - private and personal documents which were not created or received in pursuance of the EDPB's institutional or legal obligations or in the transaction of business of the EDPB or EDPB Secretariat;
  - documents legitimately belonging to the separate spaces of the Staff Committee;
  - records related to financial management and human resources which belong in files managed by the EDPS.
8. Some records, received by the EDPB, are at the same time records of EDPB members. Where needed and appropriate, implementing rules shall set out how such records are managed.

### 4 ROLES AND RESPONSIBILITIES

#### 4.1 The EDPB, represented by its Chair

9. The EDPB, represented by its Chair and supported by the EDPB Secretariat, has the overall responsibility to:
  - support the application of this records management decision throughout the organisation;
  - validate the specific retention list of the EDPB;
  - propose updates to this records management decision to the EDPB;
  - validate exceptions to the application of the specific retention list for specific files or records, in particular to destroy personal data entirely or redact it from records to be preserved.
10. The EDPB, represented by its Chair, may set out implementing rules, after consulting the records manager and the EDPB DPO.

11. Where the implementing rules concern EDPB records originating from EDPB members or their staff, the EDPB Chair will consult the EDPB members prior to issuing the implementing rules in question.

#### 4.2 EDPB Chair and Deputy Chairs

12. The EDPB Chair and Deputy Chairs shall ensure that any EDPB records drawn up or received by them are made available to the EDPB Secretariat for capture and further management.

#### 4.3 All EDPB staff

13. All EDPB staff shall:
  - distinguish records from non-records and personal documents in accordance with available records management guidance;
  - capture and manage EDPB records they are responsible for, including EDPB records created or received on personal devices or personal tools;
  - act in accordance with the applicable guidance in order to protect records in their custody from unauthorised access or improper use; and
  - handover all relevant records to his or her successor in a timely manner when transferring responsibility for any function, project, product, transaction or activity.

#### 4.4 EDPB members' representatives and staff

14. The EDPB members' representatives and staff shall ensure that any EDPB records drawn up or received by them are made available to the EDPB Secretariat for capture and further management.
15. Records containing 'special categories of data' in the meaning of Article 10(1) Reg. 2018/1725 / Article 9(1) GDPR shall be marked as such when they are made available to the EDPB Secretariat.
16. Records which are confidential or contain confidential information under national law, shall be marked as such when they are made available to the EDPB Secretariat.
17. Where implementing rules determine that specified records shall be treated differently, records in scope of these rules shall be marked as such when they are made available to the EDPB Secretariat.

#### 4.5 Records manager

18. The records manager shall:
  - maintain the filing plan;
  - promote and support compliance with the records management decision;
  - regularly conduct an appraisal of records and files managed by the EDPB and propose modifications to the specific retention list accordingly;
  - assist the EDPB, represented by its Chair, in developing implementing rules;
  - apply and lift 'legal holds' on files and propose exemptions from elimination prescribed by the specific retention list.

#### 4.6 Document management officer

19. The document management officer shall oversee the creation of case files and ensure EDPB staff correctly apply the records management decision when using the records management system.

### 5 PRINCIPLES GOVERNING RECORDS MANAGEMENT

20. All records created by EDPB staff, experts or consultants carrying out EDPB business-related activities are the property of the EDPB and all records received are in the custody of the EDPB Secretariat. All of these records must be handled in accordance with established records management practices.
21. To ensure its integrity, authenticity, reliability and accessibility, a record should be accompanied by relevant metadata documenting its context.
22. In accordance with Article 23.1 EDPB Rules of Procedure, the working language of the EDPB is English. This is applicable to records management, meaning that metadata and titles of files and records shall be in English.

#### 5.1 Records management systems

23. The management of EDPB records is ensured through the use of trustworthy record-keeping systems designed to capture, maintain and retrieve records while ensuring their continued integrity and authenticity.
24. A records management system does not only register records, but more broadly captures them to clearly and reliably identify them, ensure their traceability and make them available to other users through filing or other means of aggregation of records throughout their life cycle.
25. A record-keeping system must also support the disposal of records in accordance with the retention list.

#### 5.2 Capture and filing of records

26. Records shall be captured if they contain important information which is not short-lived or if they may involve action or follow-up by the EDPB.
27. To ensure that records are complete and accurate and the information they contain is reliable and authentic, records shall:
  - contain clear information on their business context (e.g. metadata such as date, title, author, product information);
  - be captured according to the business process they support and document (e.g. a specific procedure or a project) by the identified owner of the activity;
  - be captured in a format / medium compatible with standard office applications available at the EDPB;
  - be filed in corporate record-keeping systems managed and monitored by their respective application managers; and
  - be grouped together in a (case) file with records that relate to the same business activity / transaction / project / product.

28. A filing plan exists to ensure a uniform and consistent approach to filing across the EDPB.
29. Where appropriate, records shall be marked, in particular where they
  - contain 'special categories of data' in the meaning of Article 10(1) REG. 2018/1725 / Article 9(1) GDPR;
  - are confidential or contain confidential information;
  - are in scope of implementing rules determining these records shall be treated differently.

### 5.3 Storage and Preservation

30. The captured records shall not be altered. They may be removed or replaced by subsequent versions until the file they belong to is closed.
31. The content of records and their relevant metadata must be readable throughout their period of storage by any person authorised to have access to them.

### 5.4 Retention, transfer and elimination

32. The administrative retention period for the various categories of files and, in certain cases, records, is set out in the specific retention lists of the EDPB, drawn up on the basis of the organisational context, the existing legislation, accountability requirements and the risk associated with keeping or disposing of records at any particular point in time. Records shall be retained by the EDPB for the duration of the administrative retention period and then transferred to the European Union's historical archives or eliminated in accordance with the EDPB retention list. A set of metadata on records and files shall be retained in the original electronic repository as evidence of such records and files and their transfer or elimination.
33. The records manager shall regularly conduct an appraisal of records and files managed by the EDPB to assess whether they shall be transferred to the European Union's historical archives or eliminated.
34. To ensure in accordance with this decision that records are retained for as long as they are needed and that records authorised for elimination are destroyed safely and securely, records shall be eliminated:
  - with the assurance that they are no longer required, no work is outstanding and no litigation, audit or access request is current or pending and
  - after written approval and authorisation of the respective Head of Unit or sector responsible for the activity with a possibility to delegate this task.
35. Where all or part of a closed file is needed in the event of litigation, an investigation or a complaint to the European Ombudsman, action following expiry of the administrative retention period is suspended until the case has been dealt with ('legal hold'). Once this suspension ('legal hold') is lifted, the action scheduled following expiration of the administrative retention period can be carried out.
36. In some situations, external circumstances may justify exemption from an elimination prescribed by the retention list. Such circumstances could include the uncovering of past maladministration, an extraordinary public interest in the information or in the records concerned, or other factors that could make it necessary to preserve the files, at least temporarily.

## 5.5 Access to records

37. Access to EDPB records shall be regulated. Restrictions on access are applied to external third parties and the general public.<sup>8</sup> Decisions on granting access shall reflect the legal and other rights of the EDPB, its stakeholders and any other counterparts that might be affected by its actions.

## 5.6 Records Management and Personal Data

38. The records management decision shall support the compliance with Regulation (EU) 2018/1725 and help to protect personal data and the privacy of individuals. In particular, regarding the management of records which contain personal data, it shall be ensured that they are processed only for the purpose for which they were originally collected, for other compatible purposes or for archiving purposes in the public interest.
39. Personal data shall be kept for no longer than is necessary for the purposes for which they were originally collected, for other compatible purposes or for archiving purposes in the public interest. For this reason, the retention period of records containing personal data should be set based on a careful evaluation of how long it is strictly necessary to retain the personal data in order to fulfil its purposes. Records containing personal data may be retained for a longer period without applying a data protection retention period in case they are anonymised, i.e. kept in a form which no longer permits the identification of the concerned individuals.
40. The EDPB represented by its Chair, may decide, where appropriate, to reduce retention periods established by the records management decision to ensure compliance with the above mentioned legislation. In particular, the EDPB may decide to destroy personal data entirely or redact it from records to be preserved.

## 5.7 Information security

41. Records, files, information systems and archives, including their networks and means of transmission, shall be protected by appropriate security measures.

\*\*\*

This decision becomes applicable on 20/09/2023.

For the European Data Protection Board

The Chair

(Anu Talus)

---

<sup>8</sup> See in particular Regulation (EC) No 1049/2001 regarding public access to European Parliament, Council and Commission documents.

## Report of the work undertaken by the ChatGPT Taskforce

23 May 2024

## Table of contents

DISCLAIMER.....	3
1 Background .....	4
2 ONGOING INVESTIGATIONS.....	5
3 PRELIMINARY VIEWS .....	6
3.1 Lawfulness.....	6
3.1.1 Collection of training data, pre-processing of the data and training .....	6
3.1.2 ChatGPT input, output and training.....	7
3.2 Fairness .....	7
3.3 Transparency and information obligations.....	8
3.4 Data Accuracy.....	8
3.5 Rights of the data subject .....	9
4 ANNEX (QUESTIONNAIRE).....	9

## DISCLAIMER

The positions presented in this document result from the coordination of the members of the ChatGPT taskforce with a view to handling investigations regarding the service ChatGPT provided by the US based company OpenAI OpCo, LLC. They reflect the common denominator agreed by the Supervisory Authorities in their interpretation of the applicable provisions of the GDPR in relation to the matters that are within the scope of their investigations. The positions presented in this document do not prejudge the analysis that will have to be made by the Supervisory Authorities in each investigation respectively. In particular, it must be taken into account that the circumstances of the investigations may change over time.

## 1 BACKGROUND

1. In the recent past, numerous large language models (hereinafter “LLMs”) have emerged for use in various fields.<sup>1</sup> While these models can offer great benefits to the public, processing operations associated with LLMs shall comply with the GDPR. It has to be noted that LLMs are trained and enhanced using a huge amount of data, including personal data.
2. Some of the most popular and widely known LLMs are those in the “GPT” category,<sup>2</sup> since it has been the first consumer-facing model to be launched on 30 November 2022 through the ChatGPT service. Several Supervisory Authorities (hereinafter “SAs”) have initiated data protection investigations pursuant to Article 58(1)(a) and (b) GDPR against OpenAI OpCo, LLC (hereinafter “OpenAI”) as controller for processing operations carried out in the context of the ChatGPT service.<sup>3</sup>
3. Until 15 February 2024, OpenAI did not have an establishment in the European Union.<sup>4</sup> Insofar, as no cooperation procedures according to the One-Stop-Shop (hereinafter “OSS”) mechanism under the GDPR could apply, the European Data Protection Board (hereinafter “EDPB”) on 13 April 2023 decided to establish a taskforce to foster cooperation and exchange information on possible enforcement actions on the processing of personal data in the context of ChatGPT (hereinafter “ChatGPT TF”, SAs participating in the ChatGPT TF are hereinafter referred to as “TF members”). As the OSS did not apply, it was in particular necessary to coordinate national cases.
4. In the Plenary meeting of the EDPB on 16 January 2024, the decision was made to specify the mandate of the task force and to publish a report, outlining the interim results of the ChatGPT TF. According to this mandate, the taskforce shall:
  - Exchange information between SAs on engagement with OpenAI and on-going enforcement activities concerning ChatGPT.
  - Facilitate coordination of external communication by SAs concerning enforcement activities in the context of ChatGPT.
  - Swiftly identify a list of issues on which a common approach is needed in the context of different enforcement actions concerning ChatGPT by SAs.
5. Considering the confidential nature of the investigations, this report refers to public available information as additional source to provide information about transparency, fairness, data accuracy and data subjects’ rights towards the public.

---

<sup>1</sup> Large language models (LLMs) are deep learning models (a subset of machine learning models) that are pre-trained using vast amounts of data. Analysing these massive datasets enables the LLM to learn probability relationships and become proficient in the grammar and syntax of one or more languages. LLMs generate coherent and context-relevant language. To put it simply, LLMs respond to human language by producing coherent text that appears human-like. Most recent LLMs such as OpenAI’s GPT models are based on a neural network architecture called a transformer model.

<sup>2</sup> GPT systems are general-purpose AI models according to the definition laid down by Article 3(63) of the EU Artificial Intelligence Act (adopted, but not yet officially published as of 23 May 2024).

<sup>3</sup> The investigations of the SAs covered the versions GTP 3.5 to GTP 4.0.

<sup>4</sup> According to the “Europe privacy policy” of OpenAI, Version 15 December 2023, effective by 15 February 2024, this is OpenAI Ireland Limited.

6. As already outlined in the priorities of the EDPB for 2024-2027, providing further guidance on the interplay between the application of the GDPR and other EU legal acts, particularly the EU Artificial Intelligence Act, holds significant importance.<sup>5</sup>
7. Nonetheless, in line with the principle of accountability stipulated in Article 5(2) and Article 24 of the GDPR, controllers processing personal data in the context of LLMs shall take all necessary steps to ensure full compliance with the requirements of the GDPR.<sup>6</sup> In particular, technical impossibility cannot be invoked to justify non-compliance with these requirements, especially considering that the principle of data protection by design set out in Article 25(1) GDPR shall be taken into account at the time of the determination of the means for processing and at the time of the processing itself.

## 2 ONGOING INVESTIGATIONS

8. OpenAI was found to have a single establishment in the European Union since 15 February 2024.<sup>7</sup> Consequently, from that date onwards, the OSS framework applies for the “cross-border processing” carried out by OpenAI and the Lead SA within the meaning of Article 56 GDPR is responsible for exercising corrective powers where required. However, this is without prejudice to ongoing investigations of the respective SAs whose subject matter involves processing operations carried out until 15 February 2024 and that concern possible infringements of non-continuing or non-continuous nature.<sup>8</sup> In this respect, these national investigations will continue to be coordinated within this TF.
9. There were several sessions of the ChatGPT TF during the reporting period. As part of the activities, a common set of questions (hereinafter, “questionnaire”) was developed, which is attached to this report as Annex. Several SAs used this questionnaire as a starting basis for their exchanges with OpenAI. The development of the questionnaire aimed to promote a coordinated approach to the investigations.
10. The privacy policies in the versions prior to 15 February 2024 are within the scope of the investigations of the respective SAs. It has to be noted that OpenAI updated their “EEA privacy policy” on 15 December 2023, effective by 15 February 2024.<sup>9</sup>
11. Furthermore, it has to be noted that OpenAI has already implemented a set of measures in order to comply *inter alia* with the Italian SA’s urgent decision issuing a temporary ban with reference to the ChatGPT service in Italy and the subsequent decision to lift the temporary limitation adopted on 11 April 2023.<sup>10</sup>

---

<sup>5</sup> [https://www.edpb.europa.eu/our-work-tools/our-documents/strategy-work-programme/edpb-strategy-2024-2027\\_en](https://www.edpb.europa.eu/our-work-tools/our-documents/strategy-work-programme/edpb-strategy-2024-2027_en) (last accessed on 23 May 2024).

<sup>6</sup> Regarding the principle of accountability see para 19 of this Report.

<sup>7</sup> In line with the EDPB Guidelines 8/2022 on identifying a controller or processor’s lead Supervisory Authority V 2.1, it has to be noted that the relevant lead SA is not bound to the view of a controller and can question the determination of the single or main establishment where necessary.

<sup>8</sup> Regarding possible infringements of a continuing or continuous nature, the creation of a main or single establishment or its relocation from a third country to the EEA (in a procedure which was initially started without cooperation) mid-procedure allows the controller to benefit from the OSS and every pending proceeding should be transferred to the SA of the Member State in which the establishment is located. See EDPB Opinion 8/2019 on the competence of a supervisory authority in case of a change in circumstances relating to the main or single establishment, adopted on 9 July 2019, para 16, 30-32.

<sup>9</sup> <https://openai.com/policies/eu-privacy-policy/> (last accessed on 23 May 2024).

<sup>10</sup> <https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9874702#english> (last accessed on 23 May 2024).

### 3 PRELIMINARY VIEWS

12. The investigations conducted by the respective SAs are currently ongoing<sup>11</sup> and it is not yet possible to provide a full description of the results. Therefore, considerations in this report are to be regarded as preliminary view on certain aspects of the investigations.

#### 3.1 Lawfulness

13. In general, it has to be recalled that each processing of personal data must meet at least one of the conditions specified in Article 6(1) and, where applicable, the additional requirements laid out in Article 9(2) GDPR.<sup>12</sup>
14. When assessing the lawfulness, it is useful to distinguish the different stages of the processing of personal data.<sup>13</sup> In the present context, the stages can be categorised into i) collection of training data (including the use of web scraping data or reuse of datasets),<sup>14</sup> ii) pre-processing of the data (including filtering), iii) training, iv) prompts and ChatGPT output as well as v) training ChatGPT with prompts.

##### 3.1.1 Collection of training data, pre-processing of the data and training

15. The first three stages carry peculiar risks for the fundamental rights and freedoms of natural persons as “web scraping” enables the automated collection and extraction of certain information from different publicly available sources on the Internet (such as websites), which are then used for training purposes of ChatGPT.<sup>15</sup> Such information can contain personal data which encompasses various aspects of the personal life of the respective data subject. Depending on the source, the scraped data may even contain special categories of personal data within the meaning of Article 9(1) GDPR.
16. Regarding web scraping, OpenAI brought forward Article 6(1)(f) GDPR as legal basis.<sup>16</sup> It has to be recalled that the legal assessment of Article 6(1)(f) GDPR should be based on the following criteria:<sup>17</sup> i) existence of a legitimate interest, ii) necessity of processing, as the personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed and iii) balancing of interests. Fundamental rights and freedoms of data subjects on one hand and the controller’s legitimate interests on the other hand have to be evaluated and balanced carefully.<sup>18</sup> The reasonable expectations of data subjects should be taken into account in this assessment.<sup>19</sup>
17. As already stated by the former Article 29 Working Party, adequate safeguards play a special role in reducing undue impact on data subjects and can therefore change the balancing test in favor of the

---

<sup>11</sup> As described in para 8 of this Report.

<sup>12</sup> Judgement of the Court of Justice of 21 December 2023, C-667/21 (*Medizinischer Dienst*), para 79.

<sup>13</sup> Regarding different stages of processing of personal data see Judgement of the Court of Justice of 29 July 2019, C-40/17 (*Fashion ID*), para 70.

<sup>14</sup> For the purpose of this Report, the word “web scraping” covers both technical definitions of web scraping and web crawling.

<sup>15</sup> For the purpose of this Report, it does not make a difference whether the entity scrapes personal data itself or acquires “scraped personal data” from a third party.

<sup>16</sup> <https://help.openai.com/en/articles/7842364-how-chatgpt-and-our-language-models-are-developed> (last accessed on 23 May 2024).

<sup>17</sup> Judgement of the Court of Justice of 4 July 2023, C-252/21 (*Bundeskartellamt*), para 106.

<sup>18</sup> EDPB Guidelines 3/2019 on processing of personal data through video devices V2.0, adopted 29 January 2020, para 17-40.

<sup>19</sup> Recital 47 GDPR.

controller.<sup>20</sup> While the assessment of the lawfulness is still subject to pending investigations, such safeguards could *inter alia* be technical measures, defining precise collection criteria and ensuring that certain data categories are not collected or that certain sources (such as public social media profiles) are excluded from data collection. Furthermore, measures should be in place to delete or anonymise personal data that has been collected via web scraping before the training stage.

18. Regarding the processing of special categories of personal data, one of the exceptions of Article 9(2) must be applicable in addition, for the processing to be lawful. In principle, one of these exceptions can be Article 9(2)(e) GDPR. However, the mere fact that personal data is publicly accessible does not imply that “the data subject has manifestly made such data public”. In order to rely on the exception laid down in Article 9(2)(e) GDPR, it is important to ascertain whether the data subject had intended, explicitly and by a clear affirmative action, to make the personal data in question accessible to the general public.<sup>21</sup>
19. In the present context, where large amounts of personal data are collected via web scraping, a case-by-case examination of each data set is hardly possible. However, the aforementioned safeguards can contribute to meeting the requirements of the GDPR. For example, those measures should involve filtering data categories falling under Article 9(1) GDPR. The filtering should apply to both, data collection (for example, selecting criteria for what data is collected) and immediately after data collection (deleting data). In line with Article 5(2) and Article 24 GDPR, the burden of proof for demonstrating the effectiveness of such measures lies with OpenAI as controller.<sup>22</sup>

### 3.1.2 ChatGPT input, output and training

20. The next stages concern ChatGPT input (including “prompts”), output and training.
21. Prompts refer to the input of data subjects when interacting with LLMs such as ChatGPT as well as file uploads and the user feedback regarding the quality of the data output<sup>23</sup> (the responses) of ChatGPT. OpenAI qualifies this as “Content” and publicly states to use this information to train and improve the model. In this context, Article 6(1)(f) GDPR is brought forward as legal basis.<sup>24</sup> OpenAI provides the option to opt-out of the use of “Content” for training purposes.
22. Data subjects should, in any case, be clearly and demonstrably informed that such “Content” may be used for training purposes. This circumstance is a factor to be taken into account in the context of the balancing of interests according to Article 6(1)(f) GDPR.<sup>25</sup>

## 3.2 Fairness

23. It has to be recalled that the principle of fairness pursuant to Article 5(1)(a) GDPR 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 subject.<sup>26</sup> A crucial aspect

---

<sup>20</sup> 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, 844/14/EN, pages 31 and 42.

<sup>21</sup> Judgement of the Court of Justice of 4 July 2023, C-252/21 (*Bundeskartellamt*), para 77.

<sup>22</sup> Judgement of the Court of Justice of 14 December 2023, C-340/21 (*VB*), para 55.

<sup>23</sup> Regarding data output and the principle of data accuracy, see para 29 to para 31 of this Report.

<sup>24</sup> “Europe privacy policy” of OpenAI, Version 15 December 2023, effective by 15 February 2024, para 2 and 8.

<sup>25</sup> The TF members refer to the considerations regarding the balancing of interests in para 16 of this Report.

<sup>26</sup> EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0, adopted 20 October 2020, para 69.

of fairness is that there should be no risk transfer, meaning that controllers should not transfer the risks of the enterprise to data subjects.<sup>27</sup>

24. With regard to ChatGPT, this means that the responsibility for ensuring compliance with GDPR should not be transferred to data subjects, for example by placing a clause in the Terms and Conditions that data subjects are responsible for their chat inputs.
25. Rather, if ChatGPT is made available to the public, it should be assumed that individuals will sooner or later input personal data. If those inputs then become part of the data model and, for example, are shared with anyone asking a specific question, OpenAI remains responsible for complying with the GDPR and should not argue that the input of certain personal data was prohibited in first place.
26. OpenAI already presented measures they put in place to address these issues.<sup>28</sup> However, it has to be recalled that the examination of those measures is subject to pending investigations at this point of time.

### 3.3 Transparency and information obligations

27. When web scraping personal data from publicly accessible sources such as websites, the requirements of Article 14 GDPR apply. Considering large amounts of data is collected via web scraping, it is usually not practicable or possible to inform each data subject about the circumstances. Therefore, the exemption pursuant Article 14(5)(b) GDPR could apply, as long as all requirements of this provision are fully met.<sup>29</sup>
28. Contrary to this, when personal data is collected while directly interacting with ChatGPT, the requirements of Article 13 GDPR apply. In this context, it is of particular importance to inform data subjects that the aforementioned “Content” (the user input) may be used for training purposes.

### 3.4 Data Accuracy

29. In relation to the principle of data accuracy pursuant to Article 5(1)(d) GDPR, a difference should be made between input and output data. Input data can encompass either data collected, for instance, through web scraping or the “Content” provided by data subjects when using ChatGPT (such as “prompts”).<sup>30</sup> Output data encompasses the output following the interactions with ChatGPT.
30. It has to be noted that the purpose of the data processing is to train ChatGPT and not necessarily to provide factually accurate information. As a matter of fact, due to the probabilistic nature of the system, the current training approach leads to a model which may also produce biased or made up outputs. In addition, the outputs provided by ChatGPT are likely to be taken as factually accurate by end users, including information relating to individuals, regardless of their actual accuracy. In any case, the principle of data accuracy must be complied with.<sup>31</sup>

---

<sup>27</sup> EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0, adopted 20 October 2020, para 70.

<sup>28</sup> GPT-4 technical report, Dec. 2023, Chapter 6, arXiv:2303.08774v4 and Ouyang et al: “Training language models to follow instruction with human feedback”, Mar. 2022, arXiv:2203.02155v1.

<sup>29</sup> For further guidance regarding the requirements of Article 14(5)(b) GDPR see Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, WP260 rev.01, endorsed by the EDPB.

<sup>30</sup> Regarding “Content” see para 21 of this Report.

<sup>31</sup> Judgement of the Court of Justice of 16 January 2019, C-496/17 (*Deutsche Post AG*), para 57, according to which all processing of personal data must comply with the principles relating to data quality set out in Article 5 GDPR.

31. In line with the principle of transparency pursuant to Article 5(1)(a) GDPR, it is of importance that proper information on the probabilistic output creation mechanisms and on their limited level of reliability is provided by the controller, including explicit reference to the fact that the generated text, although syntactically correct, may be biased or made up. Although the measures taken in order to comply with the transparency principle are beneficial to avoid misinterpretation of the output of ChatGPT, they are not sufficient to comply with the data accuracy principle, as recalled above.

### 3.5 Rights of the data subject

32. The GDPR defines a set of rights of data subjects, for example to access personal data and being informed on how it is processed, to delete, to rectify, or under certain conditions to transmit personal data to a third party, to restrict the processing of the data subject's data or to file a complaint to an SA.
33. OpenAI as controller provides information on how to exercise these rights in its privacy policy (European version).<sup>32</sup> In light of the complex processing situation and the factual limits for data subjects to intervene, it is imperative that data subjects can exercise their rights in an easily accessible manner.<sup>33</sup>
34. In this context, OpenAI presents the possibility for contact by email, while some rights of the data subject can be exercised through the account settings. In line with Article 12(2) and Recital 59 GDPR, the controller shall continue improving the modalities provided for facilitating the exercise of the aforementioned data subject's rights.<sup>34</sup> In particular, this relates to the fact that, at least for the time being, OpenAI suggests users to shift from rectification to erasure when rectification is not feasible due to the technical complexity of ChatGPT.<sup>35</sup>
35. As already mentioned above,<sup>36</sup> in line with Article 25(1) GDPR, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate measures 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.<sup>37</sup>

## 4 ANNEX (QUESTIONNAIRE)

36. The following set of questions was developed within the context of the ChatGPT TF and is made available to the public. It has to be noted that SAs are independent and as such, each SA was free to modify the questionnaire or to add further questions. Moreover, differences in the questions may arise due to the respective official language to be used.

### I. General

---

<sup>32</sup> "Europe privacy policy" of OpenAI, Version 15 December 2023, effective by 15 February 2024, para 6 as well as the "Privacy policy" of OpenAI, Version June 2023, para 4.

<sup>33</sup> EDPB Guidelines 01/2022 on data subject rights - Right of access V2.0, adopted 28 March 2023, para 139-142.

<sup>34</sup> It has to be recalled that restrictions of these data subject rights are only permissible under the conditions specified in the GDPR.

<sup>35</sup> "Europe privacy policy" of OpenAI, Version 15 December 2023, effective by 15 February 2024 para 6.

<sup>36</sup> Para 7 of this Report.

<sup>37</sup> For further information on this topic, see the EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0, adopted 20 October 2020.

- a) Please provide a general and short description regarding your ChatGPT software infrastructure.
- b) Please provide a contact point of OpenAI. This is to ensure that we can contact you directly (and not via [redacted]), when necessary.
- c) Please provide the contact details of your Data Protection Officer (hereinafter: "DPO").

If you have not designated a DPO, please explain why not. In this context, please elaborate why the conditions of Article 37(1) GDPR do not apply for the processing of personal data carried out with the ChatGPT software infrastructure.

- d) In line with Article 30(4) GDPR, please provide a copy of your record of processing activities. This record can be limited to the processing of personal in relation to the product subject to this data protection audit, precisely the ChatGPT software infrastructure.

In any case, based on your record of processing activities, it must be clear for the [insert] Data Protection Authority which categories of personal data are processed for which purposes in the context of the ChatGPT software. Furthermore, it must be clear if and which special categories of personal data pursuant to Article 9 GDPR as well as personal data relating to criminal convictions and offences pursuant to Article 10 GDPR are processed.

- e) In line with Article 33(5) GDPR, please provide a copy of your documentation of personal data breaches.

## II. Principles relating to processing of personal data

- a) Please describe, in a general manner, how you ensure that the principles relating to processing of personal data pursuant to Article 5(1) GDPR are complied with.

For example: Have you implemented a data protection management system (DPMS), do you carry out regular internal and/or external audits and, if applicable, is your designated DPO involved in all data protection matters? Please provide supporting documents, where applicable.

In your answer, please differentiate between the processing of personal data relating to users (individuals signing up to "ChatGPT services") and the processing of personal data collected from third parties (for example, from the Internet, via web scraping, to feed and train the algorithm).

- b) In line with Article 5(1)(b) GDPR, please describe the different purposes for which you process personal data in the context of the ChatGPT software infrastructure.

In your answer, please be precise about which data categories you process for which purposes.

If a precise description of the purposes of the processing can already be found in your record of processing activities (see question I. a) of this letter), please describe where in the record this can be found.

- c) In line with Article 5(1)(c) GDPR, please describe how you ensure that you limit the processing of personal data to what is necessary for your purposes.

- d) In line with Article 5(1)(d) GDPR, please describe how do you deal with the question of the accuracy of the personal data used and generated in the context of the ChatGPT software infrastructure?

In particular, how do you measure the accuracy of the personal data used in your language model training, testing and validation processes?

In this context, please provide the documents in which you describe the data accuracy measurement and assessment process both for the models' training, testing and validation data and for the models output.

- e) In line with Article 5(1)(e) GDPR, please describe how long you store personal data. If applicable, please provide a copy of your retention policy.

In your answer, please differentiate between the different data categories relevant for the ChatGPT software infrastructure.

If the time limits for erasure of the different categories can already be found in your record of processing activities (see question I. a) of this letter), please describe where in the record this can be found.

- f) In line with Article 5(1)(f) and Article 32 GDPR, please describe which technical and organizational measures are implemented in order to ensure appropriate security of the personal data processed in the context of the ChatGPT software infrastructure?

### III. Data Protection Impact Assessment (“DPIA”) and risk management

- a) Have you carried out a DPIA pursuant to Article 35 GDPR regarding the processing of personal data related to users and third parties in the context of the ChatGPT software infrastructure?

If so, please provide a full copy of your DPIA, as well as information when the DPIA has been carried out.

If not, please elaborate why the conditions of Article 35(1) and (3) GDPR do not apply for the processing of personal data carried out with the ChatGPT software infrastructure.

- b) If applicable, was your designated DPO involved when carrying out your DPIA pursuant to Article 35(2) GDPR?

If so, please provide a proof (for example, a copy of the statement of your DPO regarding the DPIA).

If not, please elaborate why not.

- c) Were you able to eliminate or adequately mitigate the risks identified when carrying out your DPIA?

Please provide documents as proof (for example, the copy of your risk-analysis).

If a precise description of the measures taken to eliminate or adequately mitigate the identified risks is part of your DPIA, please describe where in the DPIA this can be found.

- d) In line with Article 24(1) last sentence GDPR, which deadlines have been established for the periodic review of your DPIA?

- e) What is the age limit for the use of the ChatGPT software infrastructure and how do you ensure that these services are not used by data subjects (users) below this age limit?

IV. Lawfulness of processing

- a) Please describe from which different sources personal data are collected and then used for the training, testing and validation of the ChatGPT software infrastructure.

Please provide this information for all different stages of training and regarding the input and output through the usage by individuals.

- b) In line with Article 6(1) GDPR, please describe your legal basis (and, if applicable, your exceptions pursuant to Article 9(2) GDPR) for the processing of personal data in the context of the ChatGPT software infrastructure.

In your answer, please be precise and provide the respective legal basis for each different processing operation, in particular regarding the processing of users' personal data as opposed to processing of non-users' (third parties) personal data collected.

Please also specify whether and to what extent personal data communicated by the users via their interactions with the chatbot are used to train the AI system or for any other purposes by OpenAI, and if so, which is the applicable legal basis.

- c) Where applicable, please provide detailed information on the following and differentiate between the respective processing operations:

i) If the legal basis is consent pursuant to Article 6(1) (and possibly exceptions pursuant to Article 9(2)(a)) GDPR, please explain how consent is obtained and how the conditions for consent, in particular regarding Article 7 GDPR, are complied with.

ii) If the legal basis is the necessity for the performance of a contract pursuant to Article 6(1)(b) GDPR, please explain which contract with which content was concluded between which parties and why the processing of personal data is necessary for the performance of such contract.

Furthermore, if the legal basis is the necessity for the performance of a contract pursuant to Article 6(1)(b) GDPR, please explain which exception of Article 9(2) GDPR is additionally relied upon when special categories of personal data are processed.

iii) If the legal basis is legitimate interests pursuant to Article 6(1)(f) GDPR, please provide detailed information regarding the balancing of interest that you have carried out, in particular why you have concluded that such interests are not overridden by the interests of the data subjects.

Furthermore, if the legal basis is legitimate interests pursuant to Article 6(1)(f) GDPR, please explain which basis of Article 9(2) GDPR is additionally relied upon when special categories of personal data are processed.

iv) In case none of the above-mentioned legal basis are relied upon, please explain why another legal basis is applicable.

- d) Please explain why data subjects (users) have to enter their telephone number in addition to their email address?

Furthermore, please explain on which legal basis and for what purposes is the telephone number used and how long will the telephone number be stored by OpenAI?

- e) In line with Article 6(4) GDPR, does processing for a purpose other than that for which the personal data have been collected ("further processing") take place?

If so, please describe which data categories are concerned by this and provide a copy of your computability test pursuant to Article 6(4) GDPR.

V. Rights of the data subject and Transparency

- a) Please explain how and when the information required pursuant to Article 13 and Article 14 GDPR is provided to the data subjects.

In the light of the currently available privacy policy published on your website, please explain in particular how and when the information required pursuant to Article 14 is provided to non-users (for example, third parties' whose data are collected to train the algorithm relied upon).

Please provide screenshots (for example, of the part of your website where the data subject is informed) as well as a copy of your up-to-date privacy policy.

- b) Please explain how you ensure compliance with the rights of data subjects pursuant to Article 15 to Article 22 GDPR.

Please provide supporting documents, where applicable (for example, the copy of an internal policy dedicated to the handling of data subject requests).

- c) With particular regard to Article 17 GDPR, please explain how compliance with the right to erasure ("right to be forgotten") is ensured?

- d) With particular regard to Article 21 GDPR, how do you comply with the requests of users that object to the processing of their personal data based on legitimate interest?

- e) With particular regard to Article 22 GDPR, does automated individual decision-making, including profiling, take place?

If so, please explain how compliance with Article 22 GDPR is ensured.

- f) Do you provide information to the users of your ChatGPT software infrastructure regarding the capabilities and limitations of the model and regarding the processing of personal data through language model services? If so, how?

VI. Transfers of personal data to third countries or international organisations

- a) Please, provide a list of the data centers you use to host and provide the ChatGPT software infrastructure (for example, to process personal data related to those services).

If personal data storage or processing location depends on some criteria, please describe them.

- b) In line with Article 44 GDPR, do transfers of personal data from users of [insert country] to third countries (outside the European Union) take place?

- c) If so, which instruments are being relied on for such transfers (Article 45, Article 46 and/or Article 49 GDPR)?

Please explain in detail why you have chosen the respective instrument and how compliance with the requirement of Article 44 GDPR – namely that the level of protection of natural persons guaranteed by the GDPR is not undermined – is ensured.

Please provide documents as proof (for example, if applicable a copy of the concluded Standard Data Protection Clauses pursuant to Article 46(2)(c) GDPR). In this context, please explain if and how you follow the recommendations given in the EDPB's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

VII. Disclosure of personal data to other parties

- a) Is OpenAI the only controller pursuant to Article 4(7) GDPR for the processing of personal data in the context of the ChatGPT software infrastructure?

If so, how is it ensured that no other party (for example, another company) decides the purposes and means regarding the processing of personal data in the context of the ChatGPT software infrastructure?

If not, who are the other (joint) controllers pursuant to Article 26 GDPR? In this case, please provide a copy of your arrangement pursuant to Article 26 second sentence GDPR.

- b) For the processing of personal data in the context of the ChatGPT software infrastructure, do you have a processor pursuant to Article 28 GDPR?

If so, please provide a copy of your contract pursuant to Article 28(2) GDPR.

- c) To which third parties are the personal data processed in the context of the ChatGPT software infrastructure disclosed to (for example, a new controller who processes the personal data generated and provided by OpenAI for its own purposes) and on which legal basis pursuant to Article 6(1) and/or exception pursuant Article 9(2) GDPR?

- d) When answering the questions of Point VII, please also take into consideration the integration of the ChatGPT software infrastructure into other products, such as (but not limited to) search engines.

**Anu Talus**

Chair of the European Data Protection Board

Mr. Andres Munoz Mosquera  
ACO Office of Legal Affairs, Director  
SHAPE  
7010 Mons, Belgium

Brussels, 4 November 2024

Dear Mr. Andres Munoz Mosquera,

Thank you the kind words on my election as Chair of the European Data Protection Board that you shared in your letter of 29 April 2024, in which you also detail SHAPE's legal position and request a meeting with the EDPB to discuss data protection related matters.

As part of the international community, both NATO and the European Union are grounded in the rule of law and a commitment to uphold human rights and values, as enshrined in the EU foundational treaties and NATO's guiding principles. Further, entities that are subject to EU law must respect and adhere to the fundamental right of protection of personal data, including as reflected in secondary legislation. Therefore, entities that transfer personal data to entities in third countries or international organisations ('IOs') need to comply with Regulation 2016/679 and Regulation (EU) 2018/1725, including their rules on international transfers.

In that respect, the EDPB's 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>1</sup>, as well as additional EDPB guidance<sup>2</sup>, provide clarifications on transfers to IOs, which are also relevant for SHAPE and NATO. This for 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.

---

<sup>1</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>2</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

This being said, the EDPB is committed to continue engaging with NATO and SHAPE on the shared mission to protect human rights, including the right to privacy. In this spirit, I believe that both the EDPB and SHAPE will benefit from an open dialogue on data protection related matters. Therefore, it is my pleasure to invite you to meet the EDPB during an EDPB in-person Plenary meeting on 2–3 December 2024, 11-12 February or 8-9 April.

I would appreciate if you inform the EDPB Secretariat as soon as is practical whether either of the proposed dates is feasible for you. In that case, the EDPB Secretariat will provide further details.

Yours sincerely

Anu Talus

# Opinion of the Board (Art. 64)



**Opinion 23/2021 on the draft decision of the competent supervisory authority of Czech Republic regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR**

**Adopted on 20 July 2021**

## Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT .....	4
2.1	General reasoning of the Board regarding the submitted draft accreditation requirements	4
2.2	Analysis of the CZ SA's accreditation requirements for Code of Conduct's monitoring bodies	
	5	
2.2.1	GENERAL REMARKS .....	5
2.2.2	INDEPENDENCE .....	7
2.2.3	CONFLICT OF INTEREST .....	8
2.2.4	EXPERTISE .....	9
2.2.5	ESTABLISHED PROCEDURES AND STRUCTURES .....	9
2.2.6	TRANSPARENT COMPLAINT HANDLING .....	10
2.2.7	COMMUNICATION WITH THE CZ SA.....	10
2.2.8	REVIEW MECHANISMS .....	11
2.2.9	LEGAL STATUS .....	11
3	CONCLUSIONS / RECOMMENDATIONS .....	12
4	FINAL REMARKS.....	15

## **The European Data Protection Board**

Having regard to Article 63, Article 64 (1)(c), (3)-(8) and Article 41 (3) 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 10 and Article 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the European Data Protection Board (hereinafter “the Board”) is to ensure the consistent application of the GDPR when a supervisory authority (hereinafter “SA”) intends to approve the requirements for accreditation of a code of conduct (hereinafter “code”) monitoring body pursuant to article 41. The aim of this opinion is therefore to contribute to a harmonised approach with regard to the suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a code monitoring body by the competent supervisory authority. Even though the GDPR does not directly impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinion by: firstly, requesting the competent SAs to draft their requirements for accreditation of monitoring bodies based on article 41(2) GDPR and on the Board’s “Guidelines 1/2019 on Codes of Conduct and Monitoring bodies under Regulation 2016/679” (hereinafter the “Guidelines”), using the eight requirements as outlined in the guidelines’ accreditation section (section 12); secondly, providing the competent SAs with written guidance explaining the accreditation requirements; and, finally, requesting the competent SAs to adopt the requirements in line with this opinion, so as to achieve an harmonised approach.

(2) With reference to article 41 GDPR, the competent supervisory authorities shall adopt requirements for accreditation of monitoring bodies of approved codes. They shall, however, apply the consistency mechanism in order to allow the setting of suitable requirements ensuring that monitoring bodies carry out the monitoring of compliance with codes in a competent, consistent and independent manner, thereby facilitating the proper implementation of codes across the Union and, as a result, contributing to the proper application of the GDPR.

(3) In order for a code covering non-public authorities and bodies to be approved, a monitoring body (or bodies) must be identified as part of the code and accredited by the competent SA as being capable of effectively monitoring the code. The GDPR does not define the term “accreditation”. However, article 41 (2) of the GDPR outlines general requirements for the accreditation of the monitoring body. There are a number of requirements, which should be met in order to satisfy the competent supervisory authority to accredit a monitoring body. Code owners are required to explain and

---

<sup>1</sup> References to the “Union” made throughout this opinion should be understood as references to “EEA”.

demonstrate how their proposed monitoring body meets the requirements set out in article 41 (2) GDPR to obtain accreditation.

(4) While the requirements for accreditation of monitoring bodies are subject to the consistency mechanism, the development of the accreditation requirements foreseen in the Guidelines should take into consideration the code's sector or specificities. Competent supervisory authorities have discretion with regard to the scope and specificities of each code, and should take into account their relevant legislation. The aim of the Board's opinion is therefore to avoid significant inconsistencies that may affect the performance of monitoring bodies and consequently the reputation of GDPR codes of conduct and their monitoring bodies.

(5) In this respect, the Guidelines adopted by the Board will serve as a guiding thread in the context of the consistency mechanism. Notably, in the Guidelines, the Board has clarified that even though the accreditation of a monitoring body applies only for a specific code, a monitoring body may be accredited for more than one code, provided it satisfies the requirements for accreditation for each code.

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

## **HAS ADOPTED THE FOLLOWING OPINION:**

### **1 SUMMARY OF THE FACTS**

1. The Czech Supervisory Authority (hereinafter "CZ SA") has submitted its draft decision containing the accreditation requirements for a code of conduct monitoring body to the Board, requesting its opinion pursuant to article 64 (1)(c), for a consistent approach at Union level. The decision on the completeness of the file was taken on 25 May 2021.

### **2 ASSESSMENT**

#### **2.1 General reasoning of the Board regarding the submitted draft accreditation requirements**

2. All accreditation requirements submitted to the Board for an opinion must fully address article 41 (2) GDPR criteria and should be in line with the eight areas outlined by the Board in the accreditation section of the Guidelines (section 12, pages 21-25). The Board opinion aims at ensuring consistency and a correct application of article 41 (2) GDPR as regards the presented draft.
3. This means that, when drafting the requirements for the accreditation of a body for monitoring codes according to articles 41 (3) and 57 (1) (p) GDPR, all the SAs should cover these basic core requirements foreseen in the Guidelines, and the Board may recommend that the SAs amend their drafts accordingly to ensure consistency.

4. All codes covering non-public authorities and bodies are required to have accredited monitoring bodies. The GDPR expressly request SAs, the Board and the Commission to “encourage the drawing up of codes of conduct intended to contribute to the proper application of the GDPR, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium sized enterprises.” (article 40 (1) GDPR). Therefore, the Board recognises that the requirements need to work for different types of codes, applying to sectors of diverse size, addressing various interests at stake and covering processing activities with different levels of risk.
5. In some areas, the Board will support the development of harmonised requirements by encouraging the SA to consider the examples provided for clarification purposes.
6. When this opinion remains silent on a specific requirement, it means that the Board is not asking the CZ SA to take further action.
7. This opinion does not reflect upon items submitted by the CZ SA, which are outside the scope of article 41 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

## **2.2 Analysis of the CZ SA’s accreditation requirements for Code of Conduct’s monitoring bodies**

8. Taking into account that:
  - a. Article 41 (2) GDPR provides a list of accreditation areas that a monitoring body need to address in order to be accredited;
  - b. Article 41 (4) GDPR requires that all codes (excluding those covering public authorities per Article 41 (6)) have an accredited monitoring body; and
  - c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for monitoring bodies and conduct the accreditation of a body for monitoring codes of conduct.

the Board is of the opinion that:

### **2.2.1 GENERAL REMARKS**

9. The Board notes that the draft accreditation requirements do not follow the structure set out in Section 12 of the Guidelines. For example, the sections on “Independence” including “Accountability”, “Review mechanism” and “legal status” are missing in the draft accreditation requirements. In this regards, for the sake of clarity the Board considers that the overall structure of the document should be improved. Therefore, with the aim to facilitate the assessment and ensure consistency , the Board recommends the CZ SA to follow the structure of the Guidelines in the draft requirements and to add the missing sections .
10. The Board observes that section 8 (Application for accreditation) of the draft accreditation requirements indicates a list of evidence to support the application for accreditation, which however does not include all the requirements of the Guidelines. Therefore, the Board recommends that CZ SA include in the draft accreditation requirements examples of evidences related to all requirements.

11. In addition, with the aim to facilitate the clarity of the draft accreditation requirements, the Board encourages the CZ SA to include in the respective sections of the requirements the examples of the information or documents confirming that the relevant requirements are met.
12. The Board observes that the last paragraph of the introductory part of the CZ SA's draft accreditation requirements (page 2) refers to a code of conduct as a tool for international transfers. As part of the work program for 2020-2021, the Board is currently working on Guidelines on Codes of Conduct as a tool for transfers. Since the Guidelines have not been adopted yet, the Board considers that this reference in the draft accreditation requirements might create confusion. Therefore, the Board recommends the CZ SA to delete this section.
13. The Board notes that subsection 1.5 of the draft accreditation requirements refers to offences committed by the monitoring body or the statutory representative of the monitoring body "in connection with the line of business". Taking into account the nature of the activities of the monitoring bodies, the Board encourages the CZ SA to clarify and further elaborate on this requirement in order to ensure that the above wording refers to activities not related to monitoring functions.
14. For the sake of consistency and clarity, the Board encourages the CZ SA to replace throughout the draft accreditation requirements the term "the Office for Personal Data Protection" with the term "Competent Supervisory Authority" in line with the terminology used in the Guidelines. At the same time the Board encourages the CZ SA to introduce in the definition section of the draft requirements a definition of the term «Competent Supervisory Authority», to be understood as the Office for Personal Data Protection.
15. As regards section 2 of the accreditation requirements, the Board encourages the CZ SA to clarify that the accreditation may be reviewed periodically, to provide transparent information on what happens after the expiry of the validity of the accreditation and explain how periodic reviews will work in practice even before 5 years period of validity.
16. The Board notes that in section 2. "Monitoring agreements concluded between a monitoring body and a monitored entity" of the CZ SA draft accreditation requirements, it is stated that the relationship between the monitoring body and the code members is subject to regulation by private law agreement. The Board highlights that the binding nature of the rules of the code of conduct, including those providing for the monitoring mechanism, would result from the (mere) adhesion of the code members to the code, as well as from their membership of the representative association. Whereas contractual arrangements are not, per se, excluded, the Board is of the opinion that the essential elements of the monitoring body's function should be included in the code itself, because they are not negotiable. Additional clauses may be added in the form of an agreement or contract between the monitoring body and the code member, as long as they do not entail a variation in the essential elements of the monitoring body's function, as set out in the code. Therefore, the Board recommends the CZ SA to specify that the core elements of the monitoring body's function will be included in the code of conduct.
17. Along the same lines, under the same section, the Board also recommends deleting the relevant requirements for agreements between the monitoring body and monitored entities in section 2. of the draft accreditation requirements.
18. As regards subsection 1.3 of the draft accreditation requirements the Board recommends the CZ SA to modify this requirement in order to specify that the monitoring body shall be able to demonstrate that all processing operations, which it performs for its monitoring tasks, are compliant with the GDPR.

19. In addition, the Board encourages the CZ SA to revise the requirements in order to avoid misunderstandings stemming from the translation of the document into English (for example, in section 1.1 the term “a natural person engaged in business” should be replaced by “natural persons acting as undertaking”; section 1.5 should refer to “integrity requirements”, instead of “impeccability requirements”; the reference to the “importance and complexity of the processings” under section 6.3 should be replaced by “nature and complexity of the processings”; section 7.3 should read “complaints and petitions handling procedures », instead of “complaints and concerns handling procedures” (in the same way sections 15.1.2 and 15.1.4), as the Board understands it is a translation mistake).
20. The Board is of the opinion that subsection 9.1 and 11.1 of the CZ SA’s draft accreditation requirements consist of elements which seem not to be necessary for the performance of monitoring bodies and is unclear. Therefore, with a view to avoiding inconsistencies and ambiguities the Board encourages the CZ SA to revise these requirements accordingly.

### **2.2.2 INDEPENDENCE**

21. According to the Board, independence for a monitoring body should be understood as a series of formal rules and procedures for the appointment, terms of reference and operation of the monitoring body. In Board’s view these rules and procedures will allow the monitoring body to perform the monitoring of compliance with a code of conduct in complete autonomy, without being directly or indirectly influenced, nor subject to any form of pressure that might affect its decisions. This means that a monitoring body should not be in a position to receive any instructions regarding the exercise of its task from code members, the profession, industry or sector to which the code applies, or from the code owner itself. Therefore, the monitoring body must demonstrate impartiality and independence in relation to four main areas: legal and decision-making procedures, financial resources, organisational resources and structure and accountability. However, the Board observes that the CZ SA’s accreditation requirements do not cover entirely the four areas outlined and are not structured in line with the Guidelines. In particular, there are no specific references to the legal and decision-making procedures, organisational resources and accountability of the monitoring body. The Board recommends the CZ SA to further develop the requirements concerning independence of the monitoring body, in line with the four areas. Furthermore, the Board encourages the CZ SA to include practical examples that provide a clearer view on how the independence can be demonstrated in the four areas.
22. Furthermore, for the sake of consistency and clarity, the Board encourages the CZ SA to replace throughout the draft accreditation requirements the terms “impartiality” with the term “independence” in line with the terminology used in the Guidelines and keep the term impartiality only in the context of organizational independence of MB.
23. Taking into account definition of the monitoring body specified in the definitions section, the Board understands that the CZ SA’s draft accreditation requirements apply to both internal and external monitoring bodies. Where the monitoring body is part of the code owner organisation, particular focus must be made on their ability to act independently. The Board is of the opinion that internal monitoring bodies cannot be set up within a code member, but only within a code owner. Therefore, the Board recommends that this is clarified and reflected in the text of the draft accreditation requirements. Furthermore, the Board encourages the CZ SA to tailor the examples taking into account that monitoring bodies can be external or internal monitoring bodies.

24. The Board encourages the CZ SA to add a requirement to prove that a specific separated budget is allocated to internal monitoring bodies by the code owner.
25. The Board observes that subsection 4.2 of the CZ SA's draft accreditation requirements specifies that the monitoring body shall have "adequate resources to cover costs of liability for its activities (e.g. financial reserves, insurances)". The Board is of the opinion that this obligation could prevent small or medium monitoring bodies from getting accredited. Therefore, the Board recommends the CZ SA to either delete this requirement or to soften the wording and refer to the monitoring body's responsibilities in general.

### **2.2.3 CONFLICT OF INTEREST**

26. The Board notes that the requirements relating to the conflict of interest are partly specified in section 3. (Management of impartiality) and section 8.2.3 of the CZ SA's draft accreditation requirements. The Board recommends to redraft the above mentioned provisions in order to cover all requirements relating to conflict of interest.
27. The Board observes that there is no reference to internal monitoring bodies, which should be appropriately protected from any sort of sanctions or interference by the code owner, other relevant bodies, or members of the code, as a consequence of the fulfilment of its tasks (paragraph 68, page 23 of the Guidelines). The Board encourages the CZ SA to provide examples that include internal monitoring bodies.
28. As regards subsection 3.3 of the draft accreditation requirements, the Board encourages the CZ SA to clearly state that in order to avoid conflict of interest, the monitoring body must, in particular, be free of external (direct or indirect) influence and, therefore, it shall not seek nor take any instructions from any person or organisation.
29. As stated in the Guidelines, the independence of the monitoring body should be demonstrated in relation also to the profession, industry or sector to which the code applies (paragraph 63 of the Guidelines). Therefore, the Board recommends that the CZ SA specify this requirement in the draft accreditation requirements.
30. Moreover, the Board recommends the CZ SA to clarify that the monitoring body should have its own staff chosen by them or other body independent of the code member.
31. The Board encourages the CZ SA to add examples in the requirements in this respect. For example, employees of the monitoring body should be required to report possible conflicts of interest
32. As regards section 3.2, the Board encourages the CZ SA to re-draft this requirement in line with the Guidelines.
33. As regards subsection 8.2.3 indent 3 as follows: "the commitment of the statutory representative that the monitoring body shall avoid conflict of interest when carrying out a monitoring, it means that the monitoring body shall not carry out monitoring for the code members organizationally or financially connected to it (through ownership, management, staff, resources, financing or contracts other than the monitoring agreements, etc.)", the Board agrees that the risk of impartiality of the monitoring body may arise from a wide range of activities carried out by the monitoring body vis-à-vis code owners (especially in the situation where the monitoring body is an internal one) or other relevant bodies

of the sector concerned. However, the Board recognizes that providing non-supervisory services, purely administrative or organisational assistance or support activities may not involve a conflict of interest. Therefore the Board encourages the CZ SA to further elaborate on this requirement in line with the Guidelines and provide examples of situations where there is a conflict of interests and where there is not.

#### **2.2.4 EXPERTISE**

34. The Board agrees with the CZ SA that expertise needs to involve the subject-matter (sector) of the code, in which case the relevant requirements that must be fulfilled can be specific, based on the sector to which the code applies. In this context, the Board recommends to clarify section 6.3 that different interests involved and the risks of the processing activities addressed by the code should also be taken into account.
35. As regards subsection 6.3.1, the Board recommends to add also the reference to the experience with respect to the data protection law.
36. The Board recommends to add the term “expert” at the beginning of the subsection 6.3.3 of the draft accreditation requirements.
37. The Board observes that according to subsection 6.3.5 of the CZ SA’s draft accreditation requirements “Personnel maintain up-to date knowledge in technical and audit skills, especially in the course of changes in the legal framework, the relevant risks, the state of the art and the implementation costs of technical and organizational measures”. The Board recommends that the CZ SA modify and further clarify this requirement accordingly, including by deleting the last part of the sentence: “the implementation costs of technical and organizational measures”.

#### **2.2.5 ESTABLISHED PROCEDURES AND STRUCTURES**

38. The Board observes that the CZ SA under section 10 (Monitoring) of the draft accreditation requirements refers to the criteria to be taken into account for the assessment of the established procedures to monitor compliance of the code members with the code. However, the Board notes that the complexity and the risks refer to the code concerned and the data processing activities to which the code applies, are not part of such criteria. Therefore, the Board encourages the CZ SA to amend this section so to include the complexity and the risks referring to the code at stake and the data processing activities to which the code applies.
39. As regards subsection 10.1.2 of the draft accreditation requirements, the Board underlines that according to paragraph 72 of the Guidelines, procedures and structures to actively and effectively monitor compliance by members of the code will be required. These could include random or unannounced audits, annual inspections, regular reporting and the use of questionnaires. The monitoring procedures can be designed in different ways as long as they take into account factors such as the risks raised by the data processing in scope of the code, complaints received or specific incidents and the number of members of the code etc. Consideration could be given to the publication of audit reports as well as to the findings of periodic reporting from controllers and processors within the scope of the code. Therefore, the Board recommends to add some examples in the requirements, such as random or unannounced audits, annual inspections, regular reporting and the use of questionnaires.

In addition, it should be mentioned that the monitoring procedures can be designated in different ways as long as they take into account factors such as the risks raised by the data processing in scope of the code, complaints received or specific incidents and the number of members of the code.

### 2.2.6 TRANSPARENT COMPLAINT HANDLING

40. Regarding section 15 of the CZ SA's draft accreditation requirements, the Board acknowledges that the monitoring body should have "implemented appropriated procedure of handling complaints about infringements of the code and procedure of handling appeals against the monitoring results". In this regard, the Board notes that the CZ SA's draft accreditation requirements (subsection 15.1.4) include a timeframe for answering complaints. In this regard, the procedure shall envisage that the monitoring body has to inform the complainant with progress reports or the outcome of the complaint, within a reasonable time frame. This period could be extended when necessary, taking into account the size of the organisation under investigation, as well as the size of the investigation. Therefore, the Board recommends that the requirement is redrafted accordingly.
41. The Board notices that under section 12.1 of the CZ SA's draft accreditation requirements "The monitoring body shall prepare a list of applicable remedies together with the rules for their application". This is not in line with Article 40 (4) GDPR, which requires that the corrective measures must be determined in the code of conduct. Therefore, the Board recommends the CZ SA to add a reference to the list of sanctions set out in the code of conduct in cases of infringements of the code by a controller or processor adhering to it.
42. Moreover, the Board recommends the CZ SA to reflect in the draft requirements paragraph 77 of the Guidelines according to which "where required, the monitoring body should be able to inform the code member, the code owner, the competent SA and all concerned SAs about the measures taken and its justification without undue delay. Moreover, in the case where a Lead Supervisory Authority (LSA) for a transnational code member is identifiable, the monitoring body should also appropriately inform the LSA as to its sanctions".

### 2.2.7 COMMUNICATION WITH THE CZ SA

43. For the sake of consistency, the Board encourages the CZ SA to add in the title of the section 14 of the draft requirements the term "communication" in line with the Guidelines.
44. The Board observes that the CZ SA in its requirements, in subsection 14.1, refers to "changes that might have an impact on its ability to carry out monitoring". The Board is of the opinion that only "substantial changes" should be reported to the competent SA. Therefore, the Board recommends that the CZ SA modify this requirement so to address the reporting of any substantial changes (e.g. any changes that impact the monitoring body's ability to perform its function) to the CZ SA in the accreditation requirements.
45. Section 14. of the CZ SA's draft accreditation requirements develops several situations in which the monitoring body is obliged to notify the CZ SA. The Board considers that the information on the functioning of the monitoring body's activities (e.g., actions taken by the monitoring body) should also be available to the CZ SA upon its request, and encourages the CZ SA to include such reference under this section.

- 46. With regard to subsection 14.6 of the draft accreditation requirements, the Board notes that it refers to the obligation of the monitoring body to take action following CZ SA's findings on non-compliance with the Code. The Board encourages the CZ SA to clarify and develop this requirement accordingly, in particular with regard to the conditions, circumstances and taking into account the competences of the SA and the monitoring body.
- 47. In the opinion of the Board, subsection 14.5 of the draft accreditation requirements better fits into the section relating to the Review mechanisms. The Board encourages the CZ SA to develop and move this requirement to the relevant section of the draft accreditation requirements.
- 48. The Board observes that in the CZ SA's draft accreditation requirements there are no specific references to the requirement foreseen by paragraph 79 of the Guidelines. The Board recommends the CZ SA to ensure compliance with this requirement.

#### **2.2.8 REVIEW MECHANISMS**

- 49. The Board observes that there is no reference to the role of the monitoring body within the review mechanisms of the code. According to section 80 of the Guidelines "a code will need to set out appropriate review mechanisms to ensure that the code remains relevant and continues to contribute to the proper application of the GDPR. Review mechanisms should also be put in place to adapt to any changes in the application and interpretation of the law or where there are new technological developments which may have an impact upon the data processing carried out by its members or the provisions of the code". Therefore, the Board recommends the CZ SA to appropriately enrich this requirement.

#### **2.2.9 LEGAL STATUS**

- 50. The Board observes that the obligation of Article 41(4) of the GDPR together with the section 12.8 of the Guidelines is not reflected in the draft requirements. Therefore, the Board recommends that the CZ SA follow the Guidelines in terms of structure and develop missing section on legal status in order to specify that the monitoring body and its related governance structures need to be created in a manner that the code owners can demonstrate that the monitoring body has the appropriate standing to carry out its role under Article 41(4) of the GDPR.
- 51. The Board notes that under subsection 1.6 of the draft accreditation requirements "the monitoring body shall be established within the European Economic Area or Switzerland". The Board is of the opinion that the monitoring body requires an establishment in the EEA. This is to ensure that they can uphold data subject rights, deal with complaints and that GDPR is enforceable and also ensures supervision by the competent supervisory authority. Therefore, the Board recommends that the CZ SA remove the reference to Switzerland.
- 52. The Board underlines that the monitoring body should have financial and other resources, and the necessary procedures to ensure the monitoring body activity. Thereby, the Board encourages the CZ SA to specify that the monitoring body shall have adequate financial and other resources and the necessary procedures to ensure its functioning.
- 53. Moreover, the code of conduct itself will need to demonstrate that the operation of the code's monitoring mechanism is sustainable over time, covering worst-case scenarios, such as the monitoring body being unable to perform the monitoring function. In this regard, it would be advisable to require

that a monitoring body demonstrates that it can deliver the code of conduct's monitoring mechanism over a suitable period of time. Therefore, the Board recommends the CZ SA to explicitly require that monitoring bodies demonstrate continuity of the monitoring function over time.

54. The Board notes that the CZ SA's accreditation requirements do not refer generally to sub-contracting except for a restriction specified in subsection 3.2. The Board is of the opinion that the sub-contractors should be able to ensure the same degree of safeguards provided by the monitoring body in performing their activities, including the same level of competence and expertise. Therefore the Board recommends that the CZ SA indicate that the obligations applicable to the monitoring body are applicable in the same way to subcontractors.
55. In addition, the Board recommends that the CZ SA clarify whether the monitoring body may have recourse to subcontractors and under which terms and conditions.
56. The Board observes that under subsection 3.2 under paragraph 3 (Management of impartiality) "*the monitoring body is not allowed to outsource any activities of the monitoring body, except of using individual external auditors and technical experts for evaluation activities*". In the opinion of the Board to a limited extent and under certain conditions it is possible for the monitoring body to outsource certain activities. Therefore, the Board encourages the CZ SA to clarify in the requirements whether "any activities of the monitoring body" refer to the decision-making. Moreover, the Board recommends that the CZ SA indicate that the monitoring body remains responsible to the SA for monitoring in all cases.
57. In the opinion of the Board the monitoring body should be the ultimate responsible for all the decisions taken related to its monitoring function. Therefore, the Board encourages the CZ SA to specify that, notwithstanding the sub-contractors' responsibility and obligations, the monitoring body is always the ultimate responsible for the decision-making and for compliance.
58. Along the same lines, the Board is of the opinion that, even when subcontractors are used, the monitoring body shall ensure effective monitoring of the services provided by the contracting entity. The Board recommends the CZ SA to explicitly add this obligation in the draft accreditation requirements.
59. The Board underlines that a natural person acting as a monitoring body must demonstrate adequate resources that allow it to act as a monitoring body. The Board encourages the CZ SA to specify how in case of natural persons the necessary expertise (legal and technical) is ensured and to add a clear reference to the necessity of ensuring and documenting how the monitoring role is guaranteed over a long term and how it can deliver the code's monitoring mechanism over a suitable period of time.

### 3 CONCLUSIONS / RECOMMENDATIONS

60. The draft accreditation requirements of the Czech Supervisory Authority may lead to an inconsistent application of the accreditation of monitoring bodies and the following changes need to be made:
61. Regarding *general remarks* the Board recommends that the CZ SA:
  1. follow the structure of the Guidelines in the draft accreditation requirements and add the missing sections;
  2. include in the draft accreditation requirements examples of evidences related to all requirements;

3. delete the last paragraph under the introductory part of the draft accreditation requirements (page 2);
4. specify that the core elements of the monitoring body's function will be included in the code of conduct;
5. delete the relevant requirements for agreements between the monitoring bodies and monitored entities in section 2. of the draft accreditation requirements;
6. modify subsection 1.3 in order to specify that the monitoring body shall be able to demonstrate that all processing operations it performs for its monitoring tasks are compliant with the GDPR.

62. Regarding *independence* the Board recommends that the CZ SA:
1. further develop the requirements concerning impartiality and independence of the monitoring body, in line with the four areas;
  2. clarify that the internal monitoring body cannot be set up within a code member, but only within a code owner;
  3. either delete requirement specified in section 4.2. or soften the wording and refer to the monitoring body's responsibilities in general.
63. Regarding *conflict of interest* the Board recommends that the CZ SA:
1. redraft section 3 and subsection 8.2.3 in order to cover all requirements relating to conflict of interest;
  2. specify that the independence of the monitoring body should be demonstrated in relation also to the profession, industry or sector to which the code applies;
  3. clarify that the monitoring body should have its own staff chosen by them or other body independent of the code.
64. Regarding *expertise* the Board recommends that the CZ SA:
1. clarify section 6.3 that different interests involved and the risks of the processing activities addressed by the code should also be taken into account;
  2. add in subsection 6.3.1 reference to the experience with respect to the data protection law;
  3. add the term "expert" at the beginning of the section 6.3.3 of the draft accreditation requirements;
  4. modify and further clarify subsection 6.3.5, including deleting the last part of the sentence: "the implementation costs of technical and organizational measures".
65. Regarding *established procedures and structures* the Board recommends that the CZ SA:

1. add some examples in the requirements, such as random or unannounced audits, annual inspections, regular reporting and the use of questionnaires. In addition, it should be mentioned that the monitoring procedures can be designated in different ways as long as they take into account factors such as the risks raised by the data processing in scope of the code, complaints received or specific incidents and the number of members of the code.
66. Regarding *transparent complaint handling* the Board recommends that the CZ SA:
1. modify section 15 in order to envisage in the procedure that the monitoring body has to inform the complainant with progress reports or the outcome of the complaint, within a reasonable time frame. This period could be extended when necessary, taking into account the size of the organisation under investigation, as well as the size of the investigation;
  2. add a reference to the list of sanctions set out in the code of conduct in cases of infringements of the code by a controller or processor adhering to it;
  3. reflect in the draft accreditation requirements paragraph 77 of the Guidelines according to which “where required, the monitoring body should be able to inform the code member, the code owner, the competent SA and all concerned SAs about the measures taken and its justification without undue delay. Moreover, in the case where a Lead Supervisory Authority (LSA) for a transnational code member is identifiable, the monitoring body should also appropriately inform the LSA as to its sections.
67. Regarding *communication with the CZ SA* the Board recommends that the CZ SA:
1. modify subsection 14.1 to address the reporting of any substantial change (e.g. any change that impact the monitoring body’s ability to perform its function) to the CZ SA in the accreditation requirements;
  2. ensure compliance with the requirement specified by paragraph 79 of the Guidelines.
68. Regarding *review mechanisms* the Board recommends that the CZ SA:
1. fill in the missing parts of this requirement.
69. Regarding *legal status* the Board recommends that the CZ SA:
1. follow the Guidelines in terms of structure and develop missing section on legal status in order to specify that the monitoring body and its related governance structures need to be created in a manner that the code owners can demonstrate that the monitoring body has the appropriate standing to carry out its role under Article 41(4) of the GDPR;
  2. remove the reference to Switzerland in subsection 1.6;
  3. explicitly require that monitoring bodies demonstrate continuity of the monitoring function over time;

4. indicate that the obligations applicable to the monitoring body are applicable in the same way to subcontractors;
5. clarify whether the monitoring body may have recourse to subcontractors and on which terms and conditions;
6. indicate that the monitoring body remains responsible to the SA for monitoring in all cases;
7. explicitly add that when subcontractors are used, the monitoring body shall ensure effective monitoring of the services provided by the contracting entity.

## 4 FINAL REMARKS

70. This opinion is addressed to the Czech supervisory authority and will be made public pursuant to Article 64 (5) (b) GDPR.
71. According to Article 64 (7) and (8) GDPR, the CZ SA shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft decision. Within the same period, it shall provide the amended draft decision or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.
72. The CZ SA shall communicate the final decision to the Board for inclusion in the register of decisions, which have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

# Opinion of the Board (Art. 64)



**Opinion 24/2021 on the draft decision of the competent supervisory authority of Slovakia regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR**

**Adopted on 20 July 2021**

## Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT .....	4
2.1	General reasoning of the Board regarding the submitted draft accreditation requirements	4
2.2	Analysis of the SK SA's accreditation requirements for Code of Conduct's monitoring bodies	
	5	
2.2.1	GENERAL REMARKS .....	5
2.2.2	INDEPENDENCE .....	6
2.2.3	CONFLICT OF INTEREST .....	6
2.2.4	EXPERTISE .....	6
2.2.5	ESTABLISHED PROCEDURES AND STRUCTURES .....	7
2.2.6	TRANSPARENT COMPLAINT HANDLING .....	7
2.2.7	COMMUNICATION WITH THE SK SA.....	7
3	CONCLUSIONS / RECOMMENDATIONS.....	7
4	FINAL REMARKS.....	7

## The European Data Protection Board

Having regard to Article 63, Article 64 (1)(c), (3)-(8) and Article 41 (3) 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 10 and Article 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the European Data Protection Board (hereinafter “the Board”) is to ensure the consistent application of the GDPR when a supervisory authority (hereinafter “SA”) intends to approve the requirements for accreditation of a code of conduct (hereinafter “code”) monitoring body pursuant to article 41. The aim of this opinion is therefore to contribute to a harmonised approach with regard to the suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a code monitoring body by the competent supervisory authority. Even though the GDPR does not directly impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinion by: firstly, requesting the competent SAs to draft their requirements for accreditation of monitoring bodies based on article 41(2) GDPR and on the Board’s “Guidelines 1/2019 on Codes of Conduct and Monitoring bodies under Regulation 2016/679” (hereinafter the “Guidelines”), using the eight requirements as outlined in the guidelines’ accreditation section (section 12); secondly, providing the competent SAs with written guidance explaining the accreditation requirements; and, finally, requesting the competent SAs to adopt the requirements in line with this opinion, so as to achieve an harmonised approach.

(2) With reference to article 41 GDPR, the competent supervisory authorities shall adopt requirements for accreditation of monitoring bodies of approved codes. They shall, however, apply the consistency mechanism in order to allow the setting of suitable requirements ensuring that monitoring bodies carry out the monitoring of compliance with codes in a competent, consistent and independent manner, thereby facilitating the proper implementation of codes across the Union and, as a result, contributing to the proper application of the GDPR.

(3) In order for a code covering non-public authorities and bodies to be approved, a monitoring body (or bodies) must be identified as part of the code and accredited by the competent SA as being capable of effectively monitoring the code. The GDPR does not define the term “accreditation”. However, article 41 (2) of the GDPR outlines general requirements for the accreditation of the monitoring body. There are a number of requirements, which should be met in order to satisfy the competent supervisory authority to accredit a monitoring body. Code owners are required to explain and

---

<sup>1</sup> References to the “Union” made throughout this opinion should be understood as references to “EEA”.

demonstrate how their proposed monitoring body meets the requirements set out in article 41 (2) GDPR to obtain accreditation.

(4) While the requirements for accreditation of monitoring bodies are subject to the consistency mechanism, the development of the accreditation requirements foreseen in the Guidelines should take into consideration the code's sector or specificities. Competent supervisory authorities have discretion with regard to the scope and specificities of each code, and should take into account their relevant legislation. The aim of the Board's opinion is therefore to avoid significant inconsistencies that may affect the performance of monitoring bodies and consequently the reputation of GDPR codes of conduct and their monitoring bodies.

(5) In this respect, the Guidelines adopted by the Board will serve as a guiding thread in the context of the consistency mechanism. Notably, in the Guidelines, the Board has clarified that even though the accreditation of a monitoring body applies only for a specific code, a monitoring body may be accredited for more than one code, provided it satisfies the requirements for accreditation for each code.

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

## **HAS ADOPTED THE FOLLOWING OPINION:**

### **1 SUMMARY OF THE FACTS**

1. The Slovak Supervisory Authority (hereinafter "SK SA") has submitted its draft decision containing the accreditation requirements for a code of conduct monitoring body to the Board, requesting its opinion pursuant to article 64 (1)(c), for a consistent approach at Union level. The decision on the completeness of the file was taken on 25 May 2021.
2. [If applicable: In compliance with article 10 (2) of the Board Rules of Procedure, due to the complexity of the matter at hand, the Chair decided to extend the initial adoption period of eight weeks by a further six weeks.]

### **2 ASSESSMENT**

- 2.1 General reasoning of the Board regarding the submitted draft accreditation requirements**
3. All accreditation requirements submitted to the Board for an opinion must fully address article 41 (2) GDPR criteria and should be in line with the eight areas outlined by the Board in the accreditation section of the Guidelines (section 12, pages 21-25). The Board opinion aims at ensuring consistency and a correct application of article 41 (2) GDPR as regards the presented draft.

4. This means that, when drafting the requirements for the accreditation of a body for monitoring codes according to articles 41 (3) and 57 (1) (p) GDPR, all the SAs should cover these basic core requirements foreseen in the Guidelines, and the Board may recommend that the SAs amend their drafts accordingly to ensure consistency.
5. All codes covering non-public authorities and bodies are required to have accredited monitoring bodies. The GDPR expressly request SAs, the Board and the Commission to “encourage the drawing up of codes of conduct intended to contribute to the proper application of the GDPR, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium sized enterprises.” (article 40 (1) GDPR). Therefore, the Board recognises that the requirements need to work for different types of codes, applying to sectors of diverse size, addressing various interests at stake and covering processing activities with different levels of risk.
6. In some areas, the Board will support the development of harmonised requirements by encouraging the SA to consider the examples provided for clarification purposes.
7. When this opinion remains silent on a specific requirement, it means that the Board is not asking the SK SA to take further action.
8. This opinion does not reflect upon items submitted by the SK SA, which are outside the scope of article 41 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

## **2.2 Analysis of the SK SA’s accreditation requirements for Code of Conduct’s monitoring bodies**

9. Taking into account that:
  - a. Article 41 (2) GDPR provides a list of accreditation areas that a monitoring body need to address in order to be accredited;
  - b. Article 41 (4) GDPR requires that all codes (excluding those covering public authorities per Article 41 (6)) have an accredited monitoring body; and
  - c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for monitoring bodies and conduct the accreditation of a body for monitoring codes of conduct.

the Board is of the opinion that:

### **2.2.1 GENERAL REMARKS**

10. The Board notes that the information required to be submitted within the application for accreditation includes also “results of the code of conduct monitoring audit” (section 1.6.i). Coming from the premise that the monitoring body cannot perform the monitoring of compliance with a code of conduct before its accreditation the Board is not aware of how the monitoring might be audited prior to the accreditation of the monitoring body. Therefore, the Board encourages the SK SA to modify this requirement in a comprehensible way or to exclude it from the list of information required within the application for accreditation.

## 2.2.2 INDEPENDENCE

11. The Board recognizes the common principle that any relationship between the monitoring body and any code member is not acceptable. The Board notes that, under section 1.7.i, the SK requirements refer to “the application shall contain the written confirmation that... there exist no relationships between the monitoring body and one or several code member/s”. However, the Board considers that the way this requirement is drafted can, to some extent, be understood as that the existence of the MB relationships to (any) code members is not, in general, excluded. Therefore, the Board encourages the SK SA to modify this requirement so to make clear that this requirement refers to the relationship of the monitoring body with any code member.
12. The Board recognizes that one of the biggest risks related to the monitoring body is the risk of impartiality. The Board notes that such risk may arise not only from providing services to the code members but also from a wide range of activities carried out by the monitoring body vis-à-vis code owners (especially in the situation where the monitoring body is an internal one) or other relevant bodies of the sector concerned. On the other hand, the Board recognizes that providing non-supervisory services, purely administrative or organisational assistance or support activities may not involve a conflict of interest, as stated in the section 2.1.1.f of the draft SK accreditation requirements, provided that the impartiality of the monitoring body is not compromised. In this context, the Board encourages the SK SA to provide additional clarifications and examples of situations where there is not a conflict of interest and to revise the list of the specific examples.

## 2.2.3 CONFLICT OF INTEREST

13. The Board is of the opinion that examples help understand draft requirements. Therefore, the Board encourages the SK SA to include some additional examples into the draft accreditation requirements or into the complementary guidance to the requirements. In particular, the Board encourages the SK SA to add examples of situations that are likely to create a conflict of interest (section 3.1.d).

## 2.2.4 EXPERTISE

14. The Board notes that the minimum required education and experience of the personnel with a technical profile (set out in section 4.7.a) is limited to the field of technical/computer sciences and information system security. The Board is of the opinion that the required education and experience of the personnel with a technical profile should primarily be linked to the field of the specific sector and the particular processing activities which are the subject matter of the code of conduct. Therefore, the Board encourages the SK SA to adjust the education and experience requirement for the personnel with a technical profile taking more into account the sector and the processing activities which are the subject matter of the code of conduct.

### **2.2.5 ESTABLISHED PROCEDURES AND STRUCTURES**

15. The Board notes that the wording “information on the duration or expiration of the monitoring body” (section 2.1.2.f) may not be easy to understand. The “expiration of the monitoring body” is related to the monitoring body’s mandate which is set forth in the code of conduct.. Therefore, the Board encourages the SK SA to modify this requirement accordingly .
16. The Board recognizes that a monitoring body shall be able to demonstrate the procedures for assessing the eligibility of controllers and processors to sign up and apply the code of conduct. However, the Board considers the requirement to deliver the grounds for assessing this eligibility to the SK SA (section 5.1.a) too broad and encourages the SK SA to reduce this requirement to an appropriate level.

### **2.2.6 TRANSPARENT COMPLAINT HANDLING**

17. The Board agrees that a system of corrective measures, worked out and submitted by the monitoring body within the complaint handling procedure, has to be developed, inter alia, on the basis of corrective measures defined in the code of conduct, if the code of conduct contains such definitions. However, the wording of the SK requirements in the section 6.1.a (“... The monitoring body shall have suitable corrective measures, defined in the code of conduct...”) could be misinterpreted in the sense that the monitoring body must strictly adhere to what is defined in the code of conduct and is not obliged to develop the own consistent system of corrective measures. Therefore, the Board encourages the SK SA to rephrase the relevant requirement, in order to prevent any confusion in the interpretation of the requirement.

### **2.2.7 COMMUNICATION WITH THE SK SA**

18. In the section 7.1.e the SK SA requires that the substantial changes to the monitoring body, of which the SK SA has to be informed without undue delay, may include, inter alia, “any changes to the basis of accreditation”. The Board encourages the SK SA to clarify in its draft accreditation requirements (section 7.1.e) the notion of the “any changes to the basis of accreditation”.

## **3 CONCLUSIONS / RECOMMENDATIONS**

19. The Board has assessed the draft accreditation requirements of the SK supervisory authority and did not identify any issues which might lead to an inconsistent application of the accreditation of monitoring bodies.

## **4 FINAL REMARKS**

20. This Opinion is addressed to the SK supervisory authority and will be made public pursuant to Article 64 (5) (b) GDPR.
21. According to Article 64 (7) and (8) GDPR, the SK SA shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft decision.

Within the same period, it shall provide the amended draft decision or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

22. The SK SA shall communicate the final decision to the Board for inclusion in the register of decisions, which have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

# Opinion of the Board (Art. 64)



**Opinion 25/2021 on the draft decision of the competent supervisory authority of Lithuania regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)**

**Adopted on 20 July 2021**

## Table of contents

1	Summary of the Facts.....	4
2	Assessment.....	4
2.1	General reasoning of the EDPB regarding the submitted draft decision .....	4
2.2	Main points of focus for the assessment (art. 43.2 GDPR and Annex 1 to the EDPB Guidelines) that the accreditation requirements provide for the following to be assessed consistently: .....	5
2.2.1	PREFIX .....	6
2.2.2	GENERAL REMARKS.....	6
2.2.3	GENERAL REQUIREMENTS FOR ACCREDITATION .....	6
2.2.4	STRUCTURAL REQUIREMENTS .....	10
2.2.5	RESOURCE REQUIREMENTS .....	10
2.2.6	PROCESS REQUIREMENTS .....	11
2.2.7	MANAGEMENT SYSTEM REQUIREMENTS.....	12
2.2.8	FURTHER ADDITIONAL REQUIREMENTS .....	13
3	Conclusions / Recommendations.....	13
4	Final Remarks .....	15

## **The European Data Protection Board**

Having regard to Article 63, Article 64 (1c), (3) - (8) and Article 43 (3) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereafter “GDPR”),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,<sup>1</sup>

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

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (hereafter GDPR) throughout the European Economic Area. In compliance with Article 64.1 GDPR, the Board shall issue an opinion where a supervisory authority (SA) intends to approve the requirements for the accreditation of certification bodies pursuant to Article 43. The aim of this opinion is therefore to create a harmonised approach with regard to the requirements that a data protection supervisory authority or the National Accreditation Body will apply for the accreditation of a certification body. Even though the GDPR does not impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by encouraging SAs to draft their requirements for accreditation following the structure set out in the Annex to the EDPB Guidelines on accreditation of certification bodies, and, secondly by analysing them using a template provided by EDPB allowing the benchmarking of the requirements (guided by ISO 17065 and the EDPB guidelines on accreditation of certification bodies).

(2) With reference to Article 43 GDPR, the competent supervisory authorities shall adopt accreditation requirements. They shall, however, apply the consistency mechanism in order to allow generation of trust in the certification mechanism, in particular by setting a high level of requirements.

(3) While requirements for accreditation are subject to the consistency mechanism, this does not mean that the requirements should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB opinion is not to reach a single EU set of requirements but rather to avoid significant inconsistencies that may affect, for instance trust in the independence or expertise of accredited certification bodies.

(4) The “Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)” (hereinafter the “Guidelines”), and “Guidelines 1/2018 on certification and identifying certification criteria in accordance with article 42 and 43 of the Regulation 2016/679” will serve as a guiding thread in the context of the consistency mechanism.

(5) If a Member State stipulates that the certification bodies are to be accredited by the supervisory authority, the supervisory authority should establish accreditation requirements including, but not

---

<sup>1</sup> References to the “Union” made throughout this opinion should be understood as references to “EEA”.

limited to, the requirements detailed in Article 43(2). In comparison to the obligations relating to the accreditation of certification bodies by national accreditation bodies, Article 43 provides fewer details about the requirements for accreditation when the supervisory authority conducts the accreditation itself. In the interests of contributing to a harmonised approach to accreditation, the accreditation requirements used by the supervisory authority should be guided by ISO/IEC 17065 and should be complemented by the requirements a supervisory authority establishes pursuant to Article 43(1)(a). The EDPB notes that Article 43(2)(a)-(e) reflect and specify requirements of ISO 17065 which will contribute to consistency.<sup>2</sup>

(6) The opinion of the EDPB shall be adopted pursuant to Article 64 (1)(c), (3) & (8) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

## **HAS ADOPTED THE OPINION:**

### **1 SUMMARY OF THE FACTS**

1. The Lithuanian SA (hereinafter “LT SA”) has submitted its draft accreditation requirements under Article 43 (1) (a) to the EDPB. The file was deemed complete on 28 May 2021.
2. The LT SA will perform accreditation of certification bodies to certify using GDPR certification criteria.

### **2 ASSESSMENT**

#### **2.1 General reasoning of the EDPB regarding the submitted draft decision**

3. The purpose of this opinion is to assess the accreditation requirements developed by a SA, either in relation to ISO 17065 or a full set of requirements, for the purposes of allowing a national accreditation body or a SA, as per article 43(1) GDPR, to accredit a certification body responsible for issuing and renewing certification in accordance with article 42 GDPR. This is without prejudice to the tasks and powers of the competent SA. In this specific case, the Board notes that the LT SA is tasked by national law to carry out the accreditation of certification bodies. To this end, the LT SA has developed a set of requirements specifically for accreditation of certification bodies in conjunction with a set of certification criteria that is yet to be formally approved.
4. This assessment of LT SA’s draft accreditation requirements is aimed at examining on variations (additions or deletions) from the Guidelines and notably their Annex 1. Indeed, according to the Guidelines, following the approach provided by the Annex (where practical) is a good practice, even where supervisory authorities perform accreditation pursuant to Article 43(1)(a), as it is the case here.

---

<sup>2</sup> Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation, par. 39. Available at: [https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies\\_en](https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_en)

Furthermore, the EDPB's Opinion is also focused on all aspects that may impact on a consistent approach regarding the accreditation of certification bodies.

5. It should be noted that the aim of the Guidelines on accreditation of certification bodies is to assist the SAs while defining their accreditation requirements. The Guidelines' Annex does not constitute accreditation requirements as such. Therefore, the accreditation requirements for certification bodies need to be defined by the SA in a way that enables their practical and consistent application as required by the SA's context.
6. The Board notes that ISO standards, in particular ISO 17065, are subject to intellectual property rights, and therefore it will not make reference to the text of the related document in this Opinion. As a result, the Board decided to, where relevant, point towards specific sections of the ISO Standard, without, however, reproducing the text.
7. Finally, the Board has conducted its assessment in line with the structure foreseen in Annex 1 to the Guidelines (hereinafter "Annex"). Where this Opinion remains silent on a specific section of the LT SA's draft accreditation requirements, it should be read as the Board not having any comments and not asking the LT SA to take further action.
8. This opinion does not reflect upon items submitted by the LT SA, which are outside the scope of article 43 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

## **2.2 Main points of focus for the assessment (art. 43.2 GDPR and Annex 1 to the EDPB Guidelines) that the accreditation requirements provide for the following to be assessed consistently:**

- a. addressing all the key areas as highlighted in the Guidelines Annex and considering any deviation from the Annex.
- b. independence of the certification body
- c. conflicts of interests of the certification body
- d. expertise of the certification body
- e. appropriate safeguards to ensure GDPR certification criteria is appropriately applied by the certification body
- f. procedures for issuing, periodic review and withdrawal of GDPR certification; and
- g. transparent handling of complaints about infringements of the certification.

9. Taking into account that:
  - a. Article 43 (2) GDPR provides a list of accreditation areas that a certification body need to address in order to be accredited;
  - b. Article 43 (3) GDPR provides that the requirements for accreditation of certification bodies shall be approved by the competent Supervisory Authority;

- c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for certification bodies and may decide to conduct the accreditation of certification bodies itself;
- d. Article 64 (1) (c) GDPR provides that the Board shall issue an opinion where a supervisory authority intends to approve the accreditation requirements for a certification body pursuant to Article 43(3);

the Board is of the opinion that:

### 2.2.1 PREFIX

- 10. The Board acknowledges that the accreditation requirements drafted by the LT SA are presented as an Annex to the Description of the Procedure for Accreditation of Certification Bodies. The description of that procedure has not been provided to the EDPB since it is not a requirement for the accreditation of certification bodies *per se*.

### 2.2.2 GENERAL REMARKS

- 11. The Board notes that some terms in the LT SA's draft accreditation requirements are not used consistently with the Guidelines and the Annex, such as 'personal data protection operations' instead of 'personal data processing operations'; 'certification object' instead of 'object of certification'; 'the entity subject to certification' instead of 'the applicant' or 'the client'; 'earlier [versions]' instead of 'previous [versions]'; 'experience' instead of 'expertise'; 'conformity assessment' instead of 'evaluation'; "enable [the LT SA] to familiarize with" instead of "made fully accessible [to the SA]"; 'management body' instead of 'management system' etc. Moreover, in Section 7.1, paragraph 1, of draft accreditation requirements, the reference to Article 43(1)(b) of the GDPR and the 'additional requirements' established by the LT SA is not entirely accurate, since it is the LT SA which is competent to perform accreditation of certifications bodies pursuant to Article 43(1)(a) of the GDPR. In order to avoid confusion, the terms used should be aligned with the Guidelines and the Annex definitions, where possible, and used consistently. Therefore, with the aim to facilitate the assessment, the Board encourages the LT SA to amend the draft requirements accordingly.

### 2.2.3 GENERAL REQUIREMENTS FOR ACCREDITATION

- 12. The Board notes that, according to the general draft accreditation requirements in section 4.1.1 ("Legal responsibility"), the certification body must be able at any time to prove to the Inspectorate that "no bankruptcy proceedings have been instituted against the certification body, for example, by providing an extract from the Register of Legal Entities". However, the same clause is reproduced under the general requirements outlined in section 4.3 ("Liability and financing") with an additional reference to insolvency or liquidation proceedings along with bankruptcy. In this regard, the Board acknowledges that the aim in both cases is to make sure that the certification body is able to exercise the certification activity with full legal responsibility, including for example to pay compensations if necessary. Nevertheless, the Board encourages the LT SA to revise both requirements so as to avoid any redundancy and inconsistency.

13. With regard to section 4.1.2 (“Certification agreement”) of the LT SA’s draft accreditation requirements, the Board notes that the first paragraph states that the certification agreement shall be “in writing”. In order to ensure that electronic certification agreements are also covered, the EDPB encourages the LT SA to replace “in writing” by “in written form” or equivalent wording.
14. In paragraph 1 of the said section, it is established that the certification agreement shall require that the applicant always complies with both the general certification requirements of the Standard ISO 17065 and the certification criteria established by the certification body and approved by the LT SA in accordance with Article 43(2)(b) and Article 42(5) of the GDPR. In this regard, since certification criteria may be established by scheme owners who do not necessarily act as a certification bodies, the EDPB encourages the LT SA to amend the draft accreditation requirements by replacing the term ‘certification body’ with ‘scheme owner’. In addition, since according to Article 43(2)(b) and Article 42(5) of the GDPR , the certification bodies may be accredited to conduct certification under the criteria approved by the competent SA, or even by the Board, if those criteria are identified as suitable for common certification and result in a European Data Protection Seal, the EDPB recommends amending the requirement so as to take into account that the applicant could be required to comply with those criteria approved by the Board at Union level.
15. Also in section 4.1.2, paragraph 2, it is stated that the certification agreement shall require that the applicant provides the SA with all necessary information “including confidential information on the certification procedure to the extent that it is related to compliance with personal data protection requirements”. The Board considers that the wording of the draft requirement is not in line with the Annex - which refers to the transparency towards the SA *“with respect to the certification procedure including contractually confidential matters related to data protection compliance”* - and encourages the LT SA to redraft the requirement so as to reflect better what it is stated in the Annex.
16. Section 4.1.2, paragraph 3, of the LT SA’s draft accreditation requirements, provides that the certification agreement shall not reduce the responsibility of the applicant *“or the certification body set forth in Regulation (EU) 2016/679”*. The Board believes that the reference to the compliance of the certification body with the GDPR is not a matter that should be included in the certification agreement and encourages the LT SA to delete it.
17. In paragraph 5 of section 4.1.2, it is expected that the certification agreement shall *“establish the applicable certification criteria and methods, criteria for assessment of the certification object (including assessment if the certification body has sufficient competence within the context of assessment of the certification object), deadlines, procedures and the responsibility of the entity subject to certification to follow the deadlines and procedures related to certification or renewal thereof provided for in the agreement, the procedure established by the certification body and, where applicable, other ISO standards”*. The Board understands that for transparency reasons this requirement mentions in detail several aspects related to the certification procedure (criteria, methods, deadlines, procedures and responsibilities) going beyond those required in the Annex. However, for the sake of clarity, the Board encourages the LT SA to specify that the requirement can be met by including in the certification agreement a reference to the relevant documentation of the certification mechanism in which these aspects are described in detail.
18. Section 4.1.2 of the Annex, paragraph 8, provides that the certification agreement includes rules on the necessary precautions for the investigation of complaints. This element is not mentioned in the corresponding paragraph of section 4.1.2 of the LT SA’s draft accreditation requirements among the

issues that certification agreement shall address. Hence, the Board recommends including such element in the draft accreditation requirements in line with the Annex.

19. Section 4.1.2 of the LT SA's draft accreditation requirements, paragraph 9, stipulates that the certification agreement shall refer to the applicant's obligation to notify the certification body of any breaches of the GDPR and other legal acts regulating personal data protection found by supervisory authorities or court which may affect conformity assessment. The second part of the paragraph states that "*The afore-mentioned information shall be provided immediately after information on the detected breach becomes available to the entity subject to certification*". The Board understands that the objective of the notification is to inform the certification body only of possible breaches that are established by a supervisory authority or a court which may affect the applicant's conformity assessment. However, if this is the case, the required information could not have been reported immediately by the applicant, after a breach was detected, as envisaged by the last sentence of paragraph 9. Therefore, the Board encourages the LT SA to delete the last sentence of the paragraph in order to avoid confusion.
20. Section 4.1.2 of the Annex, point 6, prescribes that the certification agreement, with respect to 4.1.2.2 lit. c No. 1 ISO/IEC 17065/2012, shall set out the rules of validity, renewal, and withdrawal pursuant to Articles 42(7) and 43(4) of the GDPR including rules setting appropriate intervals for re-evaluation or review (regularity) in line with Article 42(7) of the GDPR. However, in section 4.1.2, paragraph 10, of the LT SA's draft accreditation requirements, it seems that the certification agreement only needs to contain a statement as to how the conformity assessment rules have to be established "*including the rules related to regular conformity reassessment or review intervals*" according to Article 42(7) of the GDPR. Hence, the Board recommends amending this clause of the draft accreditation requirements so as to align it with the Annex.
21. Regarding paragraph 11 of section 4.1.2, the Board recommends referring to the impact of the withdrawal or suspension of the certification body's accreditation, not only on the 'entity subject to certification', but also on the certified entity in line with the Annex. In the same paragraph, a reference is included to the consequences for the data subjects. However, the LT SA omitted a reference to [where applicable] "the consequences for the customer [that] should also be addressed", as stated in the Annex. The Board therefore recommends the LT SA to replace the term 'data subjects' with 'customer', in order to align this requirement with the Annex.
22. With regard to paragraph 12 of section 4.1.2, the EDPB recommends adding a reference to the applicant's obligation to notify the certification body of significant changes in the applicant's products, processes and services concerned by the certification as in section 4.1.2 of the Annex, paragraph 10. In addition, the Board encourages amending the corresponding explanatory note, so as to clarify that the examples provided therein cover such changes.
23. In relation to "Management of impartiality", the Board notes that in section 4.2, paragraph 3, the LT SAs draft accreditation requirements state that the certification body shall confirm that it is not related to the LT SA or its employees. According to the Annex the risk of impartiality for the certification body may arise from the possible connection with the customer it assesses. Therefore, the EDPB recommends the LT SA to replace the reference to the Data Protection Inspectorate or its employees with the reference to the customer.
24. In the said section, several examples of conflicts of interests or partiality of the certification body are provided. The Board welcomes the use of examples to further clarify the content of the requirements. However, some of these examples are drafted in general term, as if they were requirements, without

providing elements that may guide the assessment of specific cases falling in the situations described in the examples. In particular, the draft accreditation requirements mention the case where the "*major part of turnover of the certification body consists of income from provision of certification services*" (point 5), as well as where "*the activities of the certification body are financed by the entity subject to certification*" (point 6). Both situations described in the examples could probably concern most of the certification bodies, given that they are not adequately circumscribed.

25. First of all, with regard to the circumstances described in these examples, a situation likely to give rise to a conflict of interest could rather be when the certification body obtains a large part of its revenue from one or very few applicants/clients. More in general, these examples should be redrafted in more specific terms or included in the text of the requirements themselves along with the necessary elements to lead the assessment of specific cases by defining better their scope of application. Hence, the Board recommends the LT SA to amend the said examples accordingly, taking into account that a situation likely to give rise to a conflict of interest could be when the certification body obtains a large part of its revenue from one or very few applicants/clients.
26. Section 4.3 of the LT SA'S draft accreditation requirements on "Liability and financing" envisages that the certification body shall provide the documents supporting that it has appropriate measures to cover the obligations related to its activities and that it is financially stable. Among the examples provided in this clause, the fact that the certification body "*has no debts related to payments to the State budget, for example, a certificate issued by the State Tax Inspectorate under the Ministry of Finance of the Republic of Lithuania*" is mentioned in paragraph 3. In this regard, the Board encourages the LT SA to clarify why these financial obligations, which are unrelated to the GDPR, are included in the draft accreditation requirements. More specifically, the scope of this example should be better defined by specifying that it refers to the case in which such financial obligations are likely to affect the financial stability of the certification body or in any case its ability to provide certification services.
27. Another example, provided in the same subsection, paragraph 4, refers to the case where "*accreditation bodies, competent supervisory authorities or courts of Lithuania or other Member States have not taken final decisions on the breaches related to the certification body's activities, management of accounts in respect of the certification body itself or its personnel*". Also in this regard, the Board encourages the LT SA to specify that the example refers to the case in which such decisions are likely to affect the financial stability of the certification body or in any case its ability to provide certification services.
28. Among the said examples, paragraph 5 refers to the situation where the certification body carries out an assessment of the risk arising from the provision of certification services and its impact on the entity subject to certification and approves the measures for elimination or mitigation of the identified risk. This clause does not seem to contain an additional requirement to item 4.3. of ISO 17065, but rather it seems to complement items 4.2.3, 4.2.4, 4.2.11 of the same standard. Therefore, for the sake of clarity, the Board encourages LT SA to amend the draft accreditation requirements accordingly.
29. With respect to the publicly available information in subsection 4.6 of the LT SA'S draft accreditation requirements, the EDPB recommends complementing the reference to the "information about complaint handling procedures following Article 43(2)(d) of the GDPR" with the information about "the appeals" in line with the Annex.

## 2.2.4 STRUCTURAL REQUIREMENTS

30. The Board observes that section 5.1 of the LT SA's draft accreditation requirements ("Organisational structure and top management") refers to the appointment of "a person responsible for compliance with personal data protection requirements and information management, application of security measures who has at least 2 years of work experience in the area of personal data protection" The functions of this person seem similar to those of a data protection officer. The Board encourages the LT SA to clearly set out the functions of this person.
31. Among the documents supporting conformity with the afore-mentioned requirements it is mentioned as an example: "*the scheme or description of the organisational structure specifying the duties, responsibilities, accountability of the persons participating in the conformity assessment. This document or a separate document shall also contain information specified in subclause 5.1.3 of the Standard ISO 17065.*" The Board notes that this requirement closely reflects what is envisaged in item 5.1.2 of ISO 17065 and encourages the LT SA to better clarify that this is only an example based on ISO 17065.
32. Another example included among such documents is the "*scheme or other description establishing the persons to which information is provided and what information is provided, for example, information on possible breaches, risks of conflicts of interests, received complaints etc. This paragraph shall apply when information is provided to several persons*". According to the Board, this example is vague and abstract and risks being ambiguous. Hence, the Board encourages the LT SA to delete the example.

## 2.2.5 RESOURCE REQUIREMENTS

33. With regard to the requirements of certification body personnel, in subsection 6.1, the EDPB observes that the "*knowledge related to personal data protection legislation*" or the "*experience in the area of personal data protection*", as well as the "*expert knowledge on the certification object*", or the "*knowledge about personal data technical and organisational security data protection measures*" should be 'relevant', 'ongoing' and 'appropriate' as required in the Annex. Moreover, the "*experience in identifying and implementing data protection measure*" for the "*employees responsible for certification decisions*" should be 'significant' as in the Annex. Therefore, the Board recommends the LT SA to amend their draft requirements accordingly.
34. As for personnel with technical expertise (paragraph 4), the draft accreditation requirements prescribe that the certification body "*has to demonstrate that they improve their qualification in the respective area related to technical and audit knowledge, participation in continuous professional development programs*". In this regard, the Board encourages the LT SA to replace the term 'improve' with 'maintain' so as to align this requirement with the Annex.
35. Concerning the personnel with legal expertise, the Board encourages the LT SA to clarify that the required years of professional experience have to be relevant for the tasks they will perform.

## 2.2.6 PROCESS REQUIREMENTS

36. The Board notes that paragraph 3 of section 7.1 (“General”) of the LT SA’s draft accreditation requirements includes the obligation of the certification body to notify to the LT SA of the decisions on certificates sought, prior to issuing, renewing or withdrawing certifications and to provide the SA with a copy of the summary of the conclusion on the assessment carried out. Moreover, section 7.6 (“Certification decision”), in paragraph 2, prescribes the certification body to verify, before taking a decision on issue (renewal) of a certificate, if the SA has not initiated any investigations against the applicant showing that it does not meet the certification criteria. In this regard, paragraph 5 of section 7.2 (“Application”) already requires that information on whether an investigation is being carried out against the applicant is to be provided in the certification application.
37. The said requirements, read in conjunction with each other, seem to suggest that a supervision by the SA of certification decisions is entailed. However, on the basis of the explanations supplied by the LT SA, the Board understands that this does not mean that the SA would need to approve each and every decision of certification body. Thus, for the sake of clarity and legal certainty, the Board encourages the LT SA to clarify the aim of these requirements, specifying that they do not entail a supervision of each and every certification decision by the LT SA, but that the SA reserves the right to exercise the power to order the certification body not to issue certification, under Article 58 paragraph 2, lett. h) of the GDPR, if it is in possession of information concerning serious breaches of data protection rules and principles from which it derives that the applicant does not meet the certification criteria.
38. Paragraph 4 of section 7.2 (“Application”) states that the application to obtain the certification shall specify “*if the certification object also covers transfer of personal data to third countries*” as well as “*personal data to be transferred, its recipients and personal data security measures which shall be applied in such case*”. As part of the work program for 2020-2021, the Board is currently working on Guidelines on certifications as a tool for transfers. Since the Guidelines have not been adopted yet, the Board considers that the reference to the transfer of personal data to third countries in this requirement might create confusion and may need to be amended once the Guidelines are adopted. Therefore, the Board recommends deleting the said requirement as well as the reference to the transfer tools included in point 3 of the list of documents supporting conformity with the afore-mentioned requirement.
39. In section 7.3 (“Application review”), the Board recommends adding the obligation to have binding evaluation methods with respect to the ToE in the certification agreement as required in the Annex.
40. With respect to section 7.4 of the LT SA’s draft accreditation requirements (“Evaluation”), the Board notes that a specific reference to the use of external experts for conformity assessment is included in paragraph 3, as stated in the Annex. In this regard, the Board encourages the LT SA to include a specific reference to the use of external experts who have been recognized by the certification body. In addition, the Board considers that the draft accreditation requirements should explicitly state that the certification body will retain the responsibility for the decision-making, even when it uses external experts. Therefore, the Board recommends the LT SA to amend the draft accreditation requirements accordingly.
41. As for paragraph 5 of the afore-mentioned section, the Board recommends amending the draft accreditation requirements to clarify that the obligation to set out in the certification mechanism how to inform the customer about nonconformities is placed on the certification body and not on the

applicant. More in general, the Board encourages the LT SA to redraft the requirement so as to align the wording with the Annex.

42. In section 7.5 (“Review”) the draft accreditation requirement refers to the procedure for “*review and withdrawal of the conclusions drawn [by the certification body] in the course of the assessment in accordance with Articles 43(2) and 43(3) of Regulation (EU) 2016/679*” while the Annex mentions the procedures for “*regular review and revocation of the ... certifications pursuant to Article 43(2) and 43(3)*” of the GDPR. Thus, the Board encourages the LT SA to replace the term ‘conclusions’ with ‘certifications’.
43. According to paragraph 1 of section 7.8 of the draft accreditation requirements (“Directory of certified products”), the certification body shall publish information on, among others, the certified object (products, processes and services). In this regard, the Annex requires that the afore-mentioned information must be available internally and publicly available. Thus, the Board recommends the LT SA to amend the requirements in line with what it is stated in the Annex so as to clarify that, for instance, posting such information on a local intranet, would not comply with the requirements.
44. In paragraph 2 of section 7.10 (“Changes affecting certification”), among the changes affecting certification which must be assessed by the certification body, the LT SA’s draft accreditation requirements mention the “*major changes in the personal data processing operations which are (were) certified*”. For the sake of clarity, the Board encourages the LT SA to clarify the meaning of the said ‘major changes’ with regard to the client’s processing operations.
45. In paragraph 5 of the same section the draft accreditation requirements refer to “*decisions, opinions, guidelines, recommendations or good practices adopted by the Board*”. To cover other types of documents that may be issued by the EDPB, the Board encourages the LT SA to add “and other documents” at the end of this clause.
46. As for section 7.12 (“Records”) of the LT SA’s draft accreditation requirements, the Board recommends including a reference to the obligation of the certification body to keep all documentation complete, comprehensible, up-to-date and fit to audit so as to align the draft accreditation requirements with the Annex.

## 2.2.7 MANAGEMENT SYSTEM REQUIREMENTS

47. Paragraph 2 of chapter VIII (“Management system requirements”) of the LT SA’s draft accreditation requirements states that “the management body shall cover the requirements set forth in paragraphs 9.3.3 and 9.3.4 hereof”. The Board understands that the term the ‘management body’ be intended as the ‘management system’. However, the reference to the requirements set forth only in paragraphs 9.3.3 and 9.3.4 risks to create ambiguity. Thus, for the sake of clarity and legal certainty, the Board recommends replacing the reference to the said paragraphs with a more general reference to the implementation of all draft requirements from the previous chapters.
48. With regard to paragraph 3 of the said chapter, the Board notes that the obligation of the certification body to disclose to the LT SA the management principles and their documented implementation during the accreditation procedure is not foreseen. The Board recommends the LT SA to amend the draft requirements, by including such obligation, as stated in the Annex.

## 2.2.8 FURTHER ADDITIONAL REQUIREMENTS

49. With regard to section 9.3.1 (“Communication between the certification body and its clients”), the Board underlines that the procedures and communication structures in place between the certification body and its customer should include the “maintenance” of the documentation of tasks and responsibilities by the accredited certification body. Therefore, the Board recommends the LT SA to add this element in the draft accreditation requirements as provided in the Annex.
50. The last sentence of section 9.3.3 (“Administration of examination of complaints”) of the LT SA’s draft accreditation requirements partially reflects the obligation under the Annex. Indeed, the Board considers that the SA not only have to be informed of relevant complaints and objections, but they have to be shared with the SA. Therefore, the Board recommends the LT SA to redraft the requirement by stating that relevant complaints and objections shall be shared with the LT SA the as Annex requires. Moreover, the Board encourages the LT SAs to replace the reference to “justified complaints” by “substantiated complaints”, in order to provide more clarity.

## 3 CONCLUSIONS / RECOMMENDATIONS

51. The draft accreditation requirements of the LT Supervisory Authority may lead to an inconsistent application of the accreditation of certification bodies and the following changes need to be made:
52. Regarding ‘general requirements for accreditation’, the Board recommends that the LT SA:
  - 1) amends the draft accreditation requirement in paragraph 1 of section 4.1.2 (“Certification agreement”) so as to take into account that the applicant could be required to comply with the criteria of a common certification resulting in a European Data Protection Seal approved by the Board at Union level;
  - 2) in paragraph 8 of in section 4.1.2, includes a reference to the rules on the necessary precautions for the investigation of complaints among the issues that the certification agreement shall address;
  - 3) amends the draft accreditation requirements in paragraph 10 of section 4.1.2, so as to align it with the Annex;
  - 4) regarding paragraph 11 of section 4.1.2, refers to the impact of the withdrawal or suspension of the certification body’s accreditation on the certified entity and replaces the term ‘data subjects’ with ‘customer’, in order to align this requirement with the Annex;
  - 5) with regard to paragraph 12 of section 4.1.2, adds a reference to the applicant’s obligation to notify the certification body of significant changes in the applicant’s products, processes and services concerned by the certification as in section 4.1.2 of the Annex, paragraph 10;
  - 6) in section 4.2 (“Management of impartiality”), paragraph 3, replaces the reference to the Data Protection Inspectorate or its employees with the reference to the customer;
  - 7) redrafts the examples concerning conflicts of interests or partiality of the certification body provided in points 5 and 6 of section 4.2, in more specific terms or includes them in

the text of the requirements, along with the necessary elements to lead the assessment of specific cases by defining better their scope of application, taking into account that a situation likely to give rise to a conflict of interest could be when the certification body obtains a large part of its revenue from one or very few applicants/clients;

- 8) with respect to the publicly available information in subsection 4.6, complements the reference to the "*information about complaint handling procedures following Article 43(2)(d) of the GDPR*" with the information about 'the appeals' in line with the Annex;

53. Regarding 'resource requirements', the Board recommends that the LT SA:

- 1) amends the draft requirements of certification body personnel in subsection 6.1, in accordance with the Annex;

54. Regarding 'process requirements', the Board recommends that the LT SA:

- 1) deletes the draft accreditation requirement in paragraph 4 of section 7.2 ("Application"), as well as the reference to the transfers tools included in point 3 of the list of documents supporting conformity with the afore-mentioned requirement;
- 2) in section 7.3 ("Application review"), adds the obligation to have binding evaluation methods with respect to the ToE in the certification agreement as required in the Annex;
- 3) with respect to section 7.4 ("Evaluation"), paragraph 3, explicitly states that the certification body will retain the responsibility for the decision-making, even when it uses external experts;
- 4) as for paragraph 5 of the afore-mentioned section, clarifies that the obligation to set out in the certification mechanism how to inform the customer about nonconformities is placed on the certification body and not on the applicant;
- 5) as for paragraph 1 of section 7.8 ("Directory of certified products"), amends the draft accreditation requirements in line with what is stated in the Annex so as to clarify that, for instance, posting such information on a local intranet, would not comply with the requirements;
- 6) as for section 7.12 ("Records"), includes a reference to the obligation of the certification body to keep all documentation complete, comprehensible, up-to-date and fit to audit so as to align the draft accreditation requirements with the Annex;

55. Regarding 'management system requirements', the Board recommends that the LT SA:

- 1) in paragraph 2 of Chapter VIII ("Management system requirements"), replaces the reference to paragraphs 9.3.3 and 9.3.4 with a more general reference to the implementation of all draft requirements from the previous chapters;
- 2) with regard to paragraph 3 of the said Chapter, amends the draft accreditation requirements, by including the obligation of the certification body to disclose to the LT SA the management principles and their documented implementation during the accreditation procedure, as stated in the Annex.

56. Regarding ‘further additional requirements’, the Board recommends that the LT SA:
- 1) with regard to section 9.3.1 (“Communication between the certification body and its clients”), adds a reference to the “maintenance” of the documentation of tasks and responsibilities by the accredited certification body as provided in the Annex;
  - 2) redrafts the last sentence of section 9.3.3 (“Administration of examination of complaints”) by stating that relevant complaints and objections shall be shared with the LT SA the as Annex requires.

## 4 FINAL REMARKS

57. This Opinion is addressed to the LT Supervisory Authority and will be made public pursuant to Article 64 (5)(b) GDPR.
58. According to Article 64 (7) and (8) GDPR, the LT SA shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.
59. The LT SA shall communicate the final decision to the Board for inclusion in the register of decisions, which have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

# 2020 ANNUAL REPORT

## ENSURING DATA PROTECTION RIGHTS IN A CHANGING WORLD



# ENSURING DATA PROTECTION RIGHTS IN A CHANGING WORLD

An Executive Summary of this report, which provides an overview of key EDPB activities in 2020, is also available.

Further details about the EDPB can be found on our website at [edpb.europa.eu](http://edpb.europa.eu).

# TABLE OF CONTENTS

<b>1</b>	<b>GLOSSARY</b>	<b>9</b>	
<b>1</b>	<b>FOREWORD</b>	<b>12</b>	
<b>2</b>	<b>ABOUT THE EUROPEAN DATA PROTECTION BOARD: MISSION, TASKS AND PRINCIPLES</b>	<b>14</b>	
	2.1. MISSION	15	3.2.4. Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak
	2.2. TASKS AND DUTIES	15	3.2.5. Statement on restrictions on data subject rights in connection to the state of emergency in Member States
	2.3. GUIDING PRINCIPLES	15	3.2.6. Statement on the processing of personal data in the context of reopening of borders following the COVID-19 outbreak
<b>3</b>	<b>2020 – HIGHLIGHTS</b>	<b>16</b>	3.2.7. Statement on the data protection impact of the interoperability of contract tracing apps
	3.1. CONTRIBUTION OF THE EDPB TO THE EVALUATION OF THE GDPR	16	3.2.8. EDPB response Letters on COVID-related matters
	3.2. ISSUES RELATING TO COVID-19 RESPONSES	17	
	3.2.1. Statement on the processing of personal data in the context of the COVID-19 outbreak	17	3.3. INTERNATIONAL PERSONAL DATA FLOWS AFTER THE SCHREMS II JUDGMENT
	3.2.2. EDPB Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic	17	3.3.1. Statement on the Court of Justice of the European Union Judgment in Case C-311/18 - Data Protection Commissioner v Facebook Ireland and Maximillian Schrems
	3.2.3. Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak	18	3.3.2. Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems
			3.3.3. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

3.3.4. Recommendations 02/2020 on the European Essential Guarantees for surveillance measures

23

5.1.2. Guidelines 02/2020 on Arts. 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

29

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

30

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

30

5.1.5. Guidelines 05/2020 on consent under Regulation 2016/679

30

5.1.6. Guidelines 06/2020 on the interplay with the Second Payments Services Directive and the GDPR

30

5.1.7. Guidelines 07/2020 on the concepts of controller and processor in the GDPR

31

5.1.8. Guidelines 08/2020 on the targeting of social media users

32

5.1.9. Guidelines 09/2020 on relevant and reasoned objection under Regulation 2016/679

32

5.1.10. Guidelines 10/2020 on restrictions under Art. 23 GDPR

33

5.1.11. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data supplementary measures

34

5.1.12. Recommendations 02/2020 on the European Essential Guarantees for surveillance measures

34

# 4

## 2020 - AN OVERVIEW

### 4.1. FUNCTIONING OF THE EDPB: REVISED RULES OF PROCEDURE

25

25

### 4.2. THE EDPB SECRETARIAT

25

### 4.3. COOPERATION AND CONSISTENCY

26

4.3.1. IT communications tool (Internal Market Information system)

27

# 5

## EUROPEAN DATA PROTECTION BOARD ACTIVITIES IN 2020

### 5.1. GENERAL GUIDANCE (GUIDELINES, RECOMMENDATIONS, BEST PRACTICES)

28

28

28

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

29

5.1.13. Guidelines adopted following public consultation	34	5.6.2. Statement on the ePrivacy Regulation and the future role of Supervisory Authorities and the EDPB	45
<b>5.2. CONSISTENCY OPINIONS</b>	<b>35</b>	<b>5.7. OTHER DOCUMENTS</b>	<b>46</b>
5.2.1. Opinions on draft accreditation requirements for code of conduct monitoring bodies	36	5.7.1. Contribution of the EDPB to the evaluation of the GDPR	46
5.2.2. Opinions on draft requirements for accreditation of a certification body	37	5.7.2. Statement on privacy implications of mergers	46
5.2.3. Opinions on draft decisions regarding Binding Corporate Rules	38	5.7.3. Statement on the processing of personal data in the context of the COVID-19 outbreak	46
5.2.4. Other Opinions	38	5.7.4. Statement on restrictions on data subject rights in connection to the state of emergency in Member States	46
<b>5.3. BINDING DECISIONS</b>	<b>39</b>	5.7.5. Statement on the processing of personal data in the context of reopening of borders following the COVID-19 outbreak	47
<b>5.4. CONSISTENCY PROCEDURES</b>	<b>40</b>	5.7.6. Statement on the data protection impact of the interoperability of contact tracing apps	47
5.4.1. EDPB document on the procedure for the approval of certification criteria by the EDPB resulting in a common certification, the European Data Protection Seal	40	5.7.7. Statement on the Court of Justice of the European Union Judgment in Case C-311/18 – Data Protection Commissioner v Facebook Ireland and Maximillian Schrems	47
5.4.2. EDPB document on the procedure for the development of informal "Codes of Conduct sessions"	41	5.7.8. Information note on BCRs for Groups of undertakings / enterprises which have ICO as BCR Lead SA	47
<b>5.5. REGISTER FOR DECISIONS TAKEN BY SUPERVISORY AUTHORITIES AND COURTS ON ISSUES HANDLED IN THE CONSISTENCY MECHANISM</b>	<b>41</b>	5.7.9. Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 – Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems	48
<b>5.6. LEGISLATIVE CONSULTATION</b>	<b>45</b>	5.7.10. EDPB Document on Coordinated Enforcement Framework under Regulation 2016/679	48
5.6.1. EDPB Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic	45		

		<b>6</b>	<b>SUPERVISORY AUTHORITY ACTIVITIES IN 2020</b>	<b>54</b>
			<b>CROSS-BORDER COOPERATION</b>	<b>54</b>
5.7.11.	Statement on the protection of personal data processed in relation with the prevention of money laundering and terrorism financing	48	6.1. 6.1.1. Preliminary procedure to identify the Lead and Concerned Supervisory Authorities	54
5.7.12.	EDPB Document on Terms of Reference of the EDPB Support Pool of Experts	49	6.1.2. Database regarding cases with a cross-border component	55
5.7.13.	Pre-GDPR Binding Corporate Rules overview list	49	6.1.3. One-Stop-Shop mechanism	55
5.7.14.	Information note on data transfers under the GDPR to the United Kingdom after the transition period	49	6.1.4. One-Stop-Shop decisions	56
5.7.15.	Statement on the end of the Brexit transition period	50	6.1.5. Mutual assistance	68
			6.1.6. Joint operations	68
<b>5.8.</b>	<b>PLENARY MEETINGS AND EXPERT SUBGROUPS</b>	<b>50</b>	<b>6.2. NATIONAL CASES</b>	<b>68</b>
<b>5.9.</b>	<b>STAKEHOLDER CONSULTATION AND TRANSPARENCY</b>	<b>50</b>	6.2.1. Some relevant national cases with exercise of corrective powers	68
	5.9.1. Stakeholder events on future guidance	50	<b>6.3. SURVEY – BUDGET AND STAFF</b>	<b>82</b>
	5.9.2. Public consultations on draft guidance	51		
	5.9.3. Stakeholder survey on adopted guidance	51		
	5.9.4. Transparency and access to documents	52		
<b>5.10.</b>	<b>EXTERNAL REPRESENTATION OF THE EDPB</b>	<b>53</b>	<b>7 COORDINATED SUPERVISION COMMITTEE OF THE LARGE EU INFORMATION SYSTEMS AND OF EU BODIES, OFFICES AND AGENCIES</b>	<b>83</b>
	5.10.1. Participation of Chair and Deputy Chairs in conferences and speaking engagements	53		
	5.10.2. Participation of EDPB Staff in conferences and speaking engagements	53		
			<b>8 MAIN OBJECTIVES FOR 2021</b>	<b>85</b>
			8.1. 8.1. 2021-2023 STRATEGY	85

# 9

<b>ANNEXES</b>	<b>87</b>
9.1. GENERAL GUIDANCE ADOPTED IN 2020	87
9.2. CONSISTENCY OPINIONS ADOPTED IN 2020	88
9.3. LEGISLATIVE CONSULTATION	89
9.4. OTHER DOCUMENTS	89
9.5. LIST OF EXPERT SUBGROUPS WITH SCOPE OF MANDATES	91
 <b>CONTACT DETAILS</b>	 <b>96</b>



# Glossary

<b>Adequacy decision</b>	An implementing act adopted by the European Commission that decides that a non-EU country ensures an adequate level of protection of personal data.
<b>Binding Corporate Rules (BCRs)</b>	Data protection policies adhered to by controller or processors established in the EU for transfers of personal data to controllers or processors outside the EU within a group of undertakings or enterprises or groups of enterprises engaged in a joint economic activity.
<b>Charter of Fundamental Rights of the EU</b>	A legally binding Charter that sets out the civil, political, economic, social and cultural rights of EU citizens and residents (including the right to the protection of personal data in its Art. 8).
<b>Concerned Supervisory Authorities (CSAs)</b>	A Supervisory Authority concerned by the processing of personal data because: (a) the controller or processor is established on the territory of its Member State; (b) data subjects residing in the Member State are substantially affected by the processing; or (c) a complaint has been lodged with that Supervisory Authority.
<b>Court of Justice of the European Union (CJEU)</b>	The highest court in the EU judiciary system, which ensures uniform interpretation and application of EU law in EU Member States. It ensures those States and EU institutions abide by EU law.
<b>COVID-19 contact tracing</b>	A process to identify individuals who have been in contact with those infected by disease, such as COVID-19.
<b>Cross-border processing</b>	Either (a) processing of personal data that takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or (b) processing of personal data that 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.

<b>Data controller</b>	The natural or legal person, public authority, agency or other body that, 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 EU or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
<b>Data minimisation</b>	A principle that means that a data controller should limit the collection of personal data to what is directly adequate, relevant and limited to what is necessary to accomplish a specified purpose of the processing.
<b>Data processor</b>	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
<b>Data Protection Impact Assessment (DPIA)</b>	A privacy-related impact assessment aiming to evaluate the processing of personal data, including notably its necessity and proportionality, an assessment of the risks for the rights and freedom of individuals, and the measures envisaged to address the risks.
<b>Data Protection Officer (DPO)</b>	An expert on data protection law and practices, who operates independently within an organisation to ensure the internal application of data protection.
<b>Data subject</b>	The person whose personal data is processed.
<b>European Commission</b>	An EU institution that shapes the EU's overall strategy, proposes new EU laws and policies, monitors their implementation and manages the EU budget.
<b>European Economic Area (EEA) Member States</b>	EU Member States and Iceland, Liechtenstein and Norway.
<b>European Union (EU)</b>	An economic and political union between 27 European countries.
<b>General Data Protection Regulation (GDPR)</b>	An EU Regulation that sets out rules on the rights of data subjects, the duties of data controllers and processors processing personal data, international data transfers and the powers of Supervisory Authorities.
<b>Lead Supervisory Authority (LSA)</b>	The Supervisory Authority where the "main establishment" of a data controller or processor is based, which has the primary responsibility for dealing with a cross-border data processing activity and for coordinating any cross-border investigation.
<b>Main establishment</b>	Either (a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment; or (b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under the GDPR.

<b>One-Stop-Shop mechanism</b>	A mechanism whereby the Supervisory Authority with the “main establishment” of a controller or processor in the EU serves as the Lead Supervisory Authority to ensure cooperation between Supervisory Authorities in the case of cross-border processing.
<b>Personal data</b>	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.
<b>Processing</b>	Any operations or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
<b>Standard Contractual Clauses (SCCs)</b>	A set of contractual clauses that provide adequate safeguards for data transfers from the EU or the EEA to third countries or govern the relationship between controller and processor.
<b>Supervisory Authority (SA)</b>	An independent public supervisory body that monitors the application of the GDPR and other national laws relating to data protection, in order to protect the rights and freedoms of natural persons in relation to the processing of personal data. Also known as a Data Protection Authority (DPA).
<b>Third country</b>	A country outside the EU or EEA.



## Foreword

2020 and the COVID-19 pandemic made for a particularly challenging year. The pandemic and resultant lockdowns significantly altered how we live and work. They also drew attention to the nature of our fundamental rights and interests, not least the rights to privacy and data protection. Given the increasing presence of data-driven technologies in addressing the pandemic and its related challenges, the awareness of data protection rights among individuals and organisations has never been more critical.

It is important to note that the 2020 lockdown did not mean a slowdown of the EDPB's activities. On the contrary, the EDPB Secretariat organised a substantially higher number of EDPB meetings in response to these circumstances. The EDPB held 172 plenary and expert subgroup meetings and 96 drafting team meetings between rapporteurs drafting EDPB documents. We met more frequently (through our secured video platforms) and tackled a very heavy workload on top of what was already in our work programme for 2019 and 2020.

The EDPB worked quickly to respond to questions of how to process personal data in the context of the COVID-19 pandemic. We issued guidance on, amongst others, location and contact-tracing apps; processing health data for scientific research; restrictions on data subject rights in a state of emergency; and data processing in the context of reopening borders.

Aside from the pandemic and the data protection issues it raised, there were several major developments in the EU data protection legal sphere. The Court of Justice of the European Union's ruling in Schrems II had a significant impact on data exporters and more globally on any entity involved in international transfers of personal data. The EDPB immediately issued an FAQ document, followed later by our Recommendations for Supplementary Measures when using international transfer tools to ensure compliance with the EU level of personal data protection, which were subject to a public consultation. We received over 200 contributions from various stakeholders, showing the keen interest in the ruling and our related guidance.

In February 2020, the EDPB and national Supervisory Authorities (SAs) contributed to the European Commission's evaluation and review of the GDPR, as required by Art. 97 GDPR. Despite challenges, the EDPB is convinced that ongoing cooperation between SAs will facilitate a shared approach to data protection and establish consistent practices. We also believe it is premature to revise the GDPR at this point in time.

Our role includes contributing to the consistent interpretation of the GDPR by adopting Guidelines and Opinions. In 2020, we adopted 10 Guidelines on topics such as the concepts of controller and processor; and targeting of social media users, as well as three Guidelines in their final, post-consultation versions.

Next to providing guidance, ensuring consistency in enforcement and cooperation between national authorities is a key task of the EDPB. In 2020, we issued 32 Opinions under the Art. 64 GDPR consistency mechanism in areas with cross-border implications. Importantly, we successfully concluded the first dispute resolution procedure on the basis of Art. 65 GDPR. The EDPB also published its 'One-Stop-Shop' decision register online, which gives companies real case examples to guide their respective privacy project implementations.

We have recently adopted a new bi-annual work programme, which builds on the EDPB 2021-2023 Strategy. Some of

the guidance we included in this work programme for the next two years is aimed at further streamlining cross-border enforcement of data protection law.

All our work was made possible thanks to the ceaseless efforts of everyone within the EDPB, in spite of the challenges that came with the COVID-19 pandemic. We also welcomed the increased input and engagement from our stakeholders through the seven public consultations we carried out in 2020, virtual events, workshops and surveys.

Since May 2018, and even well before that, we have constantly been trying to improve the implementation of the GDPR to ensure that the law achieves its intended results, namely an equally high level of data protection everywhere in the EEA. As we look forward to 2021, we will strive to contribute to a common data protection culture that ensures individuals enjoy the robust protection of their data protection rights.

**Andrea Jelinek**  
Chair of the European Data Protection Board

# 2



## About the European Data Protection Board: mission, tasks and principles

The European Data Protection Board (EDPB) is an independent European body, established by the General Data Protection Regulation (GDPR), which aims to ensure the consistent application of data protection rules across the European Economic Area (EEA).

It achieves this aim by promoting cooperation between national Supervisory Authorities (SAs) and issuing general, EEA-wide guidance regarding the interpretation and application of data protection rules.

The EDPB comprises the Heads of the EU SAs and the European Data Protection Supervisor (EDPS). The European Commission and - with regard to GDPR-related matters - the European Free Trade Association Surveillance Authority - have the right to participate in the activities and meetings of the EDPB without voting rights.

The SAs of the EEA countries (Iceland, Liechtenstein and Norway) are also members of the EDPB, although they do not hold the right to vote. The EDPB is based in Brussels.

The EDPB has a [Secretariat](#), which is provided by the EDPS. A [Memorandum of Understanding](#) determines the terms of cooperation between the EDPB and the EDPS.

## 2.1. MISSION

The EDPB has adopted a [Mission Statement](#), whereby it aims to do the following:

- Ensure the consistent application of the GDPR and the Police and Criminal Justice Data Protection Directive across the EEA;
- Provide general opinions and guidance on European data protection laws to ensure the consistent interpretation of individuals' rights and obligations;
- Make binding decisions addressed to national SAs that ensure the consistent application of the GDPR;
- Act in accordance with its [Rules of Procedure](#) and [guiding principles](#).

## 2.2. TASKS AND DUTIES

The EDPB has the following tasks and duties:

- Provide general guidance (including Guidelines, Recommendations and Best Practices) to clarify the law;
- Adopt Consistency Findings in cross-border data protection cases;
- Promote cooperation and the effective exchange of information and Best Practices between national SAs;
- Advise the European Commission on any issue related to the protection of personal data and proposed legislation in the EEA.

## 2.3. GUIDING PRINCIPLES

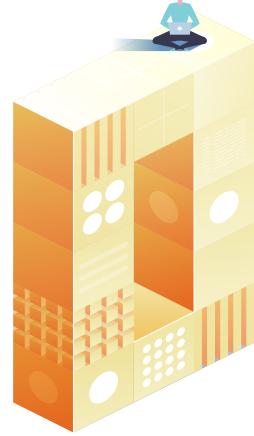
The EDPB actions are based on the following guiding principles:

- **Independence and impartiality.** The EDPB is an independent body, which performs its tasks and exercises its powers impartially;
- **Good governance, integrity and good administrative**

**behaviour.** The EDPB acts in the public interest as an expert, trustworthy and authoritative body in the field of data protection, with quality decision-making processes and sound financial management;

- **Collegiality and inclusiveness.** The EDPB acts collectively as a collegiate body pursuant to the GDPR and the Police and Criminal Justice Data Protection Directive;
- **Cooperation.** The EDPB promotes cooperation between SAs and endeavours to operate by consensus;
- **Transparency.** The EDPB operates as openly as possible to ensure efficacy and accountability to the public. The EDPB explains its activities in plain language that is accessible to all;
- **Efficiency and modernisation.** The EDPB ensures that its practices are as efficient and flexible as possible to achieve the highest level of cooperation between its members. It achieves this by using new technologies to keep working methods up to date, to minimise formalities and to provide efficient administrative support;
- **Proactivity.** The EDPB anticipates and supports innovative solutions to overcome digital challenges to data protection. The EDPB encourages close collaboration with stakeholders (whether members, observers, staff or invited experts), so that their needs and aspirations can be fully considered in its work.





## 2020 – Highlights

### 3.1. CONTRIBUTION OF THE EDPB TO THE EVALUATION OF THE GDPR

In February 2020, the EDPB and national Supervisory Authorities (SAs) contributed to the European Commission's evaluation and review of the GDPR, as required by Art. 97 GDPR.

The EDPB considers that the GDPR has strengthened data protection as a fundamental right and harmonised the interpretation of data protection principles. Data subject rights have been reinforced and data subjects are increasingly aware of the modalities to exercise their data protection rights. The GDPR also contributes to an increased global visibility of the EU legal framework and is being considered a role model outside of the EU. The EDPB believes that the GDPR's application have been successful, but acknowledges that a

number of challenges still remain. For example, insufficient resources for SAs are still a concern, as are inconsistencies in national procedures that have an impact on the cooperation mechanism between SAs.

Despite these challenges, the EDPB is convinced that ongoing cooperation between SAs will facilitate a common data protection culture and establish consistent practices.

Furthermore, the EDPB believes it is premature to revise the GDPR.

## 3.2. ISSUES RELATING TO COVID-19 RESPONSES

During the COVID-19 pandemic, EEA Member States began taking measures to monitor, contain and mitigate the spread of the virus. Many of these measures involved the processing of personal data, such as contact-tracing apps, the use of location data or the processing of health data for research purposes. As such, the EDPB offered guidance on how to process personal data in the context of the COVID-19 pandemic.

### 3.2.1. Statement on the processing of personal data in the context of the COVID-19 outbreak

The EDPB emphasises that respecting data protection rules does not hinder the fight against the COVID-19 pandemic. Even in exceptional times, controllers and processors must ensure the protection of personal data.

The GDPR allows controllers to rely on several legal grounds for lawfulness of processing and enables competent public authorities and employers to lawfully process personal data in the context of a pandemic, in accordance with national law and the conditions set therein.

All measures implemented to manage the emergency should consider data protection principles, including purpose limitation, transparency, integrity and confidentiality.

When it comes to the use of mobile location data, the EDPB stresses that public authorities should first seek to process anonymous data, to which the GDPR does not apply. When this is not possible, national legislative measures safeguarding public security can be enacted by Member States, putting in place adequate safeguards (ePrivacy Directive). The proportionality principle should also guide public authorities in the use of mobile location data. This foregrounds anonymous solutions over intrusive measures, such as the “tracking” of individuals,

which are proportional under exceptional circumstances and need to be subject to enhanced scrutiny to ensure the respect of data protection principles. The data minimisation principle should guide employers in the request and disclosure of health information in the context of COVID-19, meaning the least possible information should be disclosed to achieve a stated purpose.

Adopted: 20 March 2020

### 3.2.2. EDPB Letter concerning the European Commission’s draft Guidance on apps supporting the fight against the COVID-19 pandemic

In its draft Guidance on apps supporting the fight against the COVID-19 pandemic, the European Commission proposed the development of a pan-European and coordinated approach in the use of such tools. The EDPB welcomes this initiative, recognising that no one-size-fits-all solution applies. SAs must be consulted during the elaboration and implementation of these measures to ensure that personal data is processed lawfully and respects individuals’ rights.

Addressing specifically the use of apps for contact-tracing and warning individuals, the EDPB strongly supports the European Commission’s proposal for the voluntary adoption of such apps to foster individual trust. This does not mean that personal data processing in this context must rely on an individual’s consent, since other legal bases are available to public authorities. Contact-tracing apps should be able to discover events (i.e. contacts with COVID-19-positive people) without requiring location tracking of individual users. Both a so-called centralised and a so-called decentralised approach could be possible, provided that adequate security measures are in place.

Fully automated processes should be avoided through the strict supervision of qualified personnel, limiting the occurrence of false positives and negatives, and forms of stigmatisation.

Adopted: 14 April 2020

### 3.2.3. 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 GDPR's provisions that allow the processing of personal data for the purpose of scientific research are applicable also in the context of the COVID-19 pandemic. The Guidelines address urgent legal questions on the processing of health data for scientific research in the context of the pandemic. They address the following issues:

- **Legal basis.** Researchers should be aware that if explicit consent is used as the lawful basis for processing, all the conditions in Arts. 4(11), 6(1)(a), 7 and 9(2)(a) GDPR must be fulfilled. National legislators may enact specific laws to enable the processing of health data for scientific research purposes, pursuant to Arts. 6(1)(e) or (f) GDPR in combination with Arts. 9(2)(i) or (j) GDPR;
- **Data protection principles.** Considering the processing risks in the context of the COVID-19 outbreak, strong emphasis must be placed on the integrity and confidentiality of the data, the security of the processing, and the appropriate safeguards for the rights and freedoms of the data subject. It should be assessed whether a Data Protection Impact Assessment must be carried out;
- **Data subject rights.** Exceptional situations, such as the COVID-19 outbreak, do not suspend or restrict the possibility for data subjects to exercise their rights. The national legislator may allow restrictions to the data subject rights only in so far as it is strictly necessary.

Adopted: 21 April 2020

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

The EDPB believes that when processing personal data is necessary for implementing data-driven solutions in response to the COVID-19 pandemic, data protection is indispensable to build trust, create the conditions for social acceptability, and guarantee the effectiveness of these solutions. The EDPB clarifies the conditions and principles for the proportionate use of the following:

- **Location data.** The [ePrivacy Directive](#) contains specific rules allowing for the collection of location data from both electronic communication providers and the terminal equipment. Preference should be given to processing anonymised location data;
- **Contact-tracing apps.** The development of such tools should give careful consideration to the principle of data minimisation and data protection by design and by default, for example by collecting only relevant information when absolutely necessary. Data broadcasted by the apps must only include some unique and pseudonymous identifiers, generated by and specific to the application.

The EDPB provides non-exhaustive recommendations and obligations to designers and implementers of contact-tracing apps to guarantee the protection of personal data from the early design stage.

Adopted: 21 April 2020



### **3.2.5. Statement on restrictions on data subject rights in connection to the state of emergency in Member States**

When EEA Member States enter a state of emergency, such as the one brought on by the COVID-19 outbreak, the GDPR remains applicable and allows for efficient emergency response while protecting fundamental rights and freedoms.

Even in these exceptional times, the protection of personal data must be upheld in all emergency measures, including restrictions adopted at a national level. Art. 23 GDPR allows national legislators to restrict under specific circumstances the scope of some of the obligations and rights provided in the GDPR, as long as the restriction respects the essence of fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard, *inter alia*, important objectives of general public interest.

Any restriction on a right must respect the essence of that right and thus cannot be as intrusive as to void fundamental rights of their basic content.

Further, restrictions need to be introduced by way of a legislative measure, as any limitation on the exercise of the rights and freedoms recognised by the EU Charter of Fundamental Rights must be “provided for by law”. In particular, the domestic law must be sufficiently clear, and give an adequate indication of the circumstances in and conditions under which data controllers are empowered to resort to any such restrictions.

Legislative measures that seek to restrict the scope of data subject rights must be foreseeable to the people subject to them, including with regard to their duration in time. The restrictions need to genuinely pursue an important objective of general public interest of the EU or a Member State, such as public health. Data subject rights can be restricted, but not denied.

All restrictions on data subject rights must apply only in so far as it is strictly necessary and proportionate to safeguard the general public interest objective. The restrictions need to be limited in scope and in time, and cannot suspend or postpone the application of data subject rights and the obligations of data controllers and processors without any clear limitation in time, as this would equate to a de facto blanket suspension of those rights.

National authorities contemplating restrictions under Art. 23 GDPR should consult national SAs in due time.

Adopted: 2 June 2020

### **3.2.6. Statement on the processing of personal data in the context of reopening of borders following the COVID-19 outbreak**

During the COVID-19 pandemic, many EEA Member States placed restrictions on freedom of movement within the internal market and Schengen area to mitigate the spread of the virus. On 15 June 2020, some Member States began to progressively lift these restrictions and re-open borders. In part, this was made possible by processing personal data at border crossings by, for example, administering COVID-19 tests or requesting health certificates.

The EDPB urges Member States to adopt a standardised approach to the processing of personal data in this context, emphasising that processing must be necessary and proportionate, and the measures should be based on scientific evidence. The EDPB highlights particular data protection principles to which Member States should pay special attention. It stresses the importance of prior consultation with competent SAs when Member States process personal data in this context.

Adopted: 16 June 2020

### 3.2.7. Statement on the data protection impact of the interoperability of contract tracing apps

The EDPB maintains that, without a common EEA approach in response to the COVID-19 pandemic, at least an interoperable framework should be put in place. The EDPB elaborates on the impact on the right to data protection that an interoperable implementation of contract tracing applications can entail by focusing on seven key areas:

- **Transparency.** Information on any additional personal data processing must be provided in clear and plain language to the data subject;
- **Legal basis.** Different legal bases used by different data controllers might require implementing additional measures to safeguard data subject rights related to the legal basis;
- **Controllership.** Any operations that ensure interoperability should be considered separate to prior or subsequent processing for which the parties are individual controllers or joint controllers;
- **Data subject rights.** The exercise of rights should not become more cumbersome for the data subjects;
- **Data retention and minimisation.** Common levels of data minimisation and data retention periods should be considered;
- **Information security.** Providers should consider the additional information security risk caused by the additional processing;
- **Data accuracy.** Measures should be put in place to ensure data accuracy is maintained in the interoperable system.

Adopted: 16 June 2020

### 3.2.8. EDPB response Letters on COVID-related matters

During the COVID-19 pandemic, the EDPB responded to letters from different stakeholders asking for further clarifications on COVID-19-related matters. The EDPB received letters from the following parties: public officials (including Members of the European Parliament Ďuriš Nicholsonová and Sophie in 't Veld, and the United States Mission to the European Union); civil liberties advocacy organisations (Civil Liberties Union for Europe, Access Now and the Hungarian Civil Liberties Union); and private companies (Amazon EU Sarl).

In its responses, the EDPB reiterated that data protection legislation already takes into account data processing operations that are necessary to contribute to the fight against the pandemic, and that the data protection principles need always to be upheld. Where relevant, the EDPB referred to published or future Guidelines addressing the matters in question or encouraged consultation with national SAs.

Adopted: 24 April 2020, 19 May 2020, 3 June 2020, 17 July 2020

## 3.3. INTERNATIONAL PERSONAL DATA FLOWS AFTER THE SCHREMS II JUDGMENT

On 16 July 2020, the Court of Justice of the EU (CJEU) released its judgment in *Case C-311/18 (Schrems II)*. The CJEU examined two mechanisms that allow personal data transfers from the EEA to non-EEA countries (third countries), namely, the EU-U.S. Privacy Shield and Standard Contractual Clauses (SCCs). The CJEU invalidated the adequacy decision underlying the EU-U.S. Privacy Shield, thereby rendering it invalid as a transfer mechanism. It also ruled that the European Commission's Decision 2010/87 on SCCs for the transfer of personal data to third country processors is valid, so SCCs may still be used to

enable international data transfers. This is upon the condition that the exporter (if needed, with the help of the importer), assesses, prior to the transfer, the level of protection afforded in the context of such transfers, taking into consideration both the SCCs and the relevant aspects of the legal system of the importer's country, as regards any access to the data by that third country's public authorities. The factors to be considered for this assessment are those set out, in a non-exhaustive manner, in Art. 45(2) GDPR.

The judgment has wide-ranging implications for EEA-based entities that use these mechanisms to enable personal data transfers to the U.S. and other third countries.

### **3.3.1. Statement on the Court of Justice of the European Union Judgment in Case C-311/18 - Data Protection Commissioner v Facebook Ireland and Maximillian Schrems**

The EDPB believes that the CJEU's judgment in Case C-311/18 (*Schrems II*) highlights the importance of the fundamental right to privacy in the context of the transfer of personal data to third countries and the risk for data subjects caused by possible indiscriminate access by a third country's public authorities to the personal data transferred. Standard Contractual Clauses (SCCs) must maintain a level of protection in the third country that is essentially equivalent to that in the EEA.

The EDPB notes that the judgment emphasises that the assessment of whether the SCCs can ensure in practice for the data transferred to a third country an essentially equivalent level of protection is primarily the responsibility of exporters and importers. If the SCCs by themselves cannot guarantee an essentially equivalent level of protection in the third country, the exporter will need to consider putting in place supplementary measures that fill the protection gap.

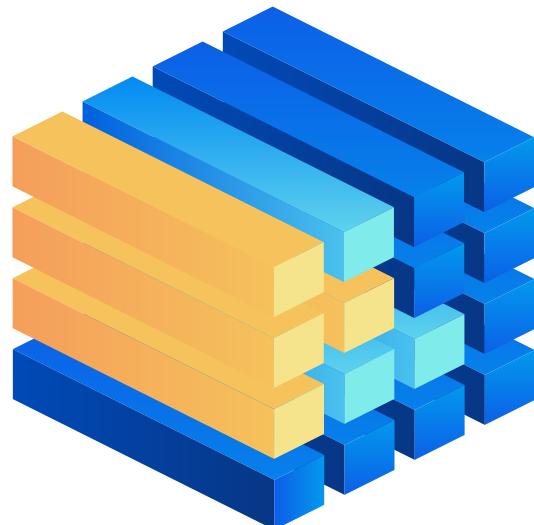
The judgment recalls and the EDPB underlines that the exporter and the importer need to comply with their obligations included in the SCCs. If they do not or cannot comply with these obligations, the exporter must suspend the transfer or terminate the agreement.

The EDPB notes that competent SAs have the duty to suspend or prohibit a personal data transfer to a third country pursuant to SCCs if they are not or cannot be complied with in that third country, and the protection of the data transferred cannot be ensured by other means, in particular where the exporter or importer has not already itself suspended or put an end to the transfer.

The EDPB recalls its position on the use of the derogations under Art. 49 GDPR, as set out in its Guidelines 02/2018, which must be applied on a case-by-case basis.

The EDPB will keep assessing the judgment and will continue providing guidance on its consequences for personal data transfers to countries outside the EEA. .

Adopted: 17 July 2020



### 3.3.2. Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems

Following the CJEU's judgment in [Case C-311/18 \(Schrems II\)](#), the EDPB provided clarifications on the judgment in a document addressing 12 Frequently Asked Questions (FAQs).

These answers stipulated that:

- There is no grace period for EEA organisations relying on the Privacy Shield to transfer personal data to the U.S.;
- As a consequence, any personal data transfers from the EEA to the U.S. are illegal if they are based on the Privacy Shield;
- The threshold set by the CJEU for transfers to the U.S. applies for any third country;
- Therefore, the CJEU's approach applies to any international data transfers relying on SCCs and, by extension, those relying on Binding Corporate Rules (BCRs) or on other Art. 46 GDPR transfer mechanisms;
- Whether or not personal data may be transferred to a third country on the basis of an Art. 46 GDPR transfer mechanism depends on the outcome of the prior assessment to be carried out by the exporter, taking into account the specific circumstances of the transfers, and the supplementary measures possibly identified. The transfer mechanism used and the supplementary measures would have to ensure that the laws of the third country of destination do not impinge on the adequate level of protection guaranteed by such mechanisms and supplementary measures;
- It is still possible to transfer personal data from the EEA to the U.S. on the basis of derogations under Art. 49 GDPR, provided the conditions set forth in this provision apply. On this provision, the EDPB refers to its Guidelines 02/2018.

SAs will cooperate within the EDPB to ensure consistency, in particular if transfers to third countries must be prohibited.

Adopted: 23 July 2020

### 3.3.3. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

The CJEU mentioned in its judgment in [Case C-311/18 \(Schrems II\)](#) the possibility for exporters of adopting supplementary measures to bring the level of protection of personal data transferred to countries outside the EEA up to the standard of essential equivalence with the EU level, where Art. 46 GDPR transfer tools cannot guarantee it by themselves. The EDPB issued Recommendations that provide data exporters with a series of six steps to follow to apply the principle of accountability to data transfers, and some examples of supplementary measures.

These steps addressed to data exporters are as follows:

- Step 1: Data exporters should know their transfers in order to be fully aware of the destination of the personal data processing and verify that personal data is adequate, relevant and limited to what is necessary in relation to the purpose for which it is transferred.
- Step 2: Data exporters should identify the transfer tools under Chapter V GDPR, which they are relying on. Relying on some tools, such as a valid adequacy decision covering the third country, will be enough to proceed with the transfer without taking any further steps, other than monitoring that the decision remains valid.

- Step 3: Data exporters should assess the laws and/or practices of the third country to determine if these could impinge on the effectiveness of the safeguards contained in the transfer tools the data exporter is relying on. This assessment should be primarily focused on third country legislation relevant to the transfer and the transfer tool relied on that could undermine its level of protection and other objective factors. The EDPB Recommendations 02/2020 on the European Essential Guarantees will be relevant in this context to evaluate the third country legislation on public authorities' access for the purpose of surveillance.
- Step 4: Data exporters should identify and adopt supplementary measures, such as various technical, contractual and organisational measures to bring the level of protection of the data transferred up to the EU standard of essential equivalence. The EDPB Recommendations 01/2020 contain in their Annex a non-exhaustive list of examples of supplementary measures with some of the conditions they would require to be effective. Data exporters must avoid, suspend or terminate the transfer to avoid compromising the level of protection of the personal data in those cases where they find no suitable supplementary measures. Data exporters should also conduct the assessment with due diligence and document it.
- Step 5: Where required, data exporters should take formal procedural steps, such as consulting competent SAs.
- Step 6: Data exporters should re-evaluate the level of protection afforded to personal data at appropriate intervals, in accordance with the principle of accountability.

Adopted: 10 November 2020



### 3.3.4. Recommendations 02/2020 on the European Essential Guarantees for surveillance measures

In light of the CJEU's judgment in [Case C-311/18 \(Schrems II\)](#), the EDPB updated the Recommendations on the European Essential Guarantees (EEG) for surveillance measures.

The Recommendations are based on the jurisprudence of the CJEU and the European Court of Human Rights. The case law from these Courts reasserts that public authorities' access, retention and further use of personal data through surveillance measures must be limited to what is strictly necessary and proportionate in a democratic society.

The Recommendations describe four EEG. The EEG are the core elements to be found when assessing the level of interference with the fundamental rights to privacy and data protection of the surveillance measures conducted by public authorities in third countries. The EEG are also part of the assessment that data exporters need to conduct to determine if a third country provides a level of protection essentially equivalent to that guaranteed within the EEA.

The EEG as updated by the Recommendations are as follows:

- Processing should be based on clear, precise and accessible rules;
- Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated;
- An independent oversight mechanism should exist;
- Effective remedies need to be available to the individual. These include providing data subjects with the possibility of bringing legal action before an independent and impartial court or body to have access to their personal data or to obtain the rectification or erasure of such data;
- A notification to the individual whose personal data has been collected or analysed must occur only to the extent that and as soon as it no longer jeopardises the tasks of public authorities.

The EEG should be assessed on an overall basis, as they are closely interlinked. These guarantees require a certain degree of interpretation, especially since the third country legislation does not have to be identical to the EU legal framework.

The assessment of third country surveillance measures may lead to one of two conclusions:

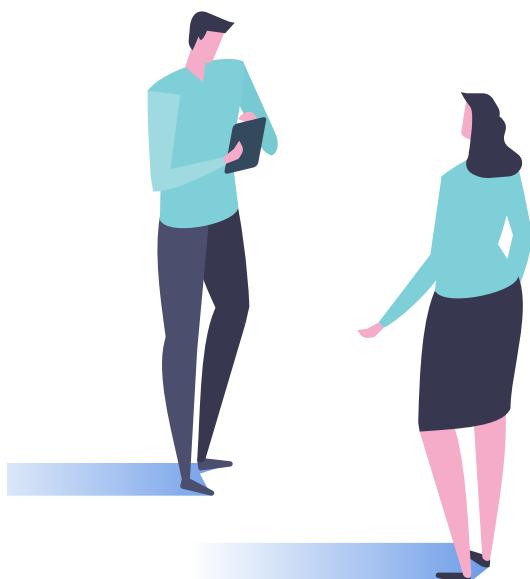
- The third country legislation at issue does not ensure the EEG requirements and thus does not provide a level of protection essentially equivalent to that guaranteed within the EEA; or
- The third country legislation at issue satisfies the EEGs.

Adopted: 10 November 2020

### **3.4. FIRST ART. 65 GDPR BINDING DECISION**

The EDPB adopted its first dispute resolution [decision](#) on the basis of Art. 65 GDPR. The binding decision addressed the dispute that arose after the Irish SA, acting as Lead SA, issued a draft decision regarding Twitter International Company and the subsequent relevant and reasoned objections expressed by a number of Concerned SAs. Section 5.3 of this Report further elaborates upon this decision.

Adopted: 9 November 2020



# 4



## 2020 - An overview

### 4.1. FUNCTIONING OF THE EDPB: REVISED RULES OF PROCEDURE

During its first plenary meeting on 25 May 2018, the EDPB adopted its Rules of Procedure (RoP), which outline the EDPB's primary operational rules, including:

- The EDPB's guiding principles;
- The EDPB's organisational framework;
- The cooperation between EDPB Members;
- The election of the Chair and Deputy Chair of the EDPB;
- The EDPB's working methods.

In January 2020, the EDPB [adopted](#) revisions to Arts. 10(1), 10(2) and 10(5) RoP and in October 2020, it [adopted](#) an amendment to Art. 11(2) RoP.

### 4.2. THE EDPB SECRETARIAT

The EDPB Secretariat, which is provided by the European Data Protection Supervisor (EDPS), offers analytical, administrative and logistical support to the EDPB. The EDPB Secretariat is in charge of drafting EDPB documents, providing IT solutions to ensure transparent communications between all the European national Supervisory Authorities (SAs), handling EDPB media relations, as well as organising all EDPB meetings.

Although staff at the EDPB Secretariat are employed by the EDPS, staff members only work under the instructions of the Chair of the EDPB. A [Memorandum of Understanding](#) establishes the terms of cooperation between the EDPB and the EDPS.

In 2020, due to limitations brought on by the COVID-19 pandemic, the EDPB Secretariat implemented novel measures to improve working conditions amidst unprecedented circumstances. These measures included: employing new videoconferencing tools; holding more frequent meetings; and implementing new initiatives to keep the EDPB Members connected, for example the addition of extra Jabber accounts and a new Wiki platform.

In light of these circumstances, the EDPB Secretariat organised a substantially increased number of EDPB meetings in 2020. The EDPB held 172 meetings, including plenary meetings and expert subgroup meetings, where ordinarily they would hold about 100 meetings. Notably, the EDPB held 27 plenary meetings, compared to 11 in previous years.

The EDPB Secretariat also led the drafting of over 60% of the Guidelines, Opinions, Recommendations and Statements adopted by the EDPB in 2020.

The EDPB designated a DPO in accordance with Art. 43 Regulation 2018/1725. The DPO's position and tasks are defined in Arts. 44 and 45 of said Regulation, and are further detailed in the EDPB [DPO Implementing Rules](#).

### 4.3. COOPERATION AND CONSISTENCY

As stated in the GDPR, the SAs of EEA Member States cooperate closely to ensure that people's data protection rights are protected consistently across the EEA. They assist each other and coordinate their decision-making in cross-border data protection cases.

Through the so-called consistency mechanism, the EDPB issues [Consistency Findings](#), comprising Opinions and Decisions (outlined in Chapter 5 of this Report), to clarify fundamental provisions of the GDPR and to ensure consistency in its application among SAs.

In 2020, the EDPB issued 32 [Opinions](#) under Art. 64 GDPR. Most of these Opinions concern draft accreditation requirements for a code of conduct monitoring body or a certification body, as well as Controller Binding Corporate Rules for various companies.

In November 2020, the EDPB adopted its first dispute resolution [decision](#) on the basis of Art. 65 GDPR to address a dispute that arose after the Irish SA, acting as Lead SA, issued a draft decision regarding Twitter International Company and the subsequent relevant and reasoned objections expressed by a number of Concerned SAs.

The EDPB also published a [register](#) of decisions taken by national SAs in line with the One-Stop-Shop cooperation procedure (Art. 60 GDPR) on its website.

In November 2020, the EDPB adopted a [document](#) on the procedure for the development of informal "Codes of Conduct sessions", in which it proposes a format for the Codes sessions. The document further elaborates on the role of SAs, and their interaction with both the competent SAs and the Code owners, as well as on the role of the EDPB Secretariat.

With increasing attention placed on the cooperation mechanism outlined in the GDPR, the EDPB in October 2020 issued [Guidelines](#) to establish a common understanding of the notion of a "relevant and reasoned" objection and to address any unfamiliarity surrounding its interpretation.

In October 2020, the EDPB released a [document](#) on the Coordinated Enforcement Framework (CEF), which provides a structure for coordinating recurring annual activities by SAs. The main objective of the CEF is to facilitate joint actions in a flexible but coordinated manner, ranging from joint awareness raising and information gathering to enforcement sweeps and joint investigations.

As part of its 2021-2023 Strategy, the EDPB decided to establish a Support Pool of Experts (SPE) on the basis of a pilot project. The goal is to provide material support to EDPB Members in the form of expertise that is useful for investigations and enforcement activities, and to enhance cooperation and solidarity between EDPB Members by sharing, reinforcing and complementing strengths and addressing operational needs. In December 2020, the EDPB adopted a [document](#) on the terms of reference of the SPE.

In July 2020, the EDPB adopted an [information note](#) with regard to arrangements to be made by BCR holders with the United Kingdom SA (UK SA) as the competent SA (BCR Lead SAs). In light of Brexit, BCR Lead SAs need to make all organisational arrangements to establish a new BCR Lead in the EEA. In December 2020, the EDPB issued a [statement](#) on the end of the Brexit transition period in which it describes the main implications of the end of this period for data controllers and processors. In particular, the EDPB underlines the issue of data transfers to a third country as well as the consequences in the area of regulatory oversight and the One-Stop-Shop mechanism. The Brexit transition period, during which the UK SA was still involved in the EDPB's administrative cooperation, expired at the end of 2020. Additionally, the EDPB adopted an [information note](#) on data transfers under the GDPR after the Brexit transition period ends.

#### **4.3.1. IT communications tool (Internal Market Information system)**

The EDPB promotes the cooperation between SAs by providing a robust IT system. Since 25 May 2018, SAs have been using the Internal Market Information (IMI) system to exchange information necessary for the GDPR cooperation and consistency mechanism in a standardised and secured way.

The European Commission's Directorate General for Internal Market, Industry, Entrepreneurship and SMEs (DG GROW) developed the IMI system. In the context of the EDPB, it was adapted in close cooperation with the EDPB Secretariat and SAs to cater to the needs of the GDPR. Since its implementation, the IMI system has proven to be an asset for SAs, which continue to use and access the system daily.

In 2020, SAs registered 628 cases in the IMI system.<sup>1</sup> They also initiated a number of procedures in the same period, described below:

- Identification of the Lead SA and Concerned SAs: 742 procedures;
- Mutual Assistance Procedures: 246 formal procedures and 2,258 informal procedures;
- One-Stop-Shop mechanism – draft decisions and final decisions: 203 draft decisions, from which 93 resulted in final decisions.

<sup>1</sup>. A case entry refers to an entry in the IMI system that allows the management of cooperation or consistency procedures from beginning to end. It is a central point where SAs can share and find information on a specific issue to facilitate the retrieval of information and the consistent application of the GDPR.

A case entry may consist of the management of multiple procedures (e.g. an Art. 60 GDPR procedure or an Art. 65 GDPR procedure in case of disagreement) or just a single one related to a case register entry. Multiple complaints on the same subject relating to the same processing can be bundled in one single case entry.



# 5



## European Data Protection Board Activities in 2020

To ensure the consistent application of the GDPR across the EEA, the EDPB issues general guidance to clarify European data protection laws.

This guidance provides the public and stakeholders with a consistent interpretation of their rights and obligations, and ensures that national Supervisory Authorities (SAs) have a benchmark for applying and enforcing the GDPR.

The EDPB is also empowered to issue Opinions or Binding Decisions to guarantee the consistent application of the GDPR by SAs. Throughout 2020, the EDPB issued multiple guidance and consistency documents, as summarised below.

### **5.1. GENERAL GUIDANCE (GUIDELINES, RECOMMENDATIONS, BEST PRACTICES)**

In 2020, the EDPB adopted several Guidelines and Recommendations on the data protection requirements pertaining to the COVID-19 pandemic (see Section 3.2 of this Report), new technologies, personal data transfers and the meaning of specific terms in the GDPR.

These Guidelines and Recommendations are summarised below.

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

As they move into the mainstream, connected vehicles have become a significant subject for regulators, particularly as they require personal data processing within a complex ecosystem.

The EDPB Guidelines aim to clarify the key privacy and data protection risks, including the security of personal data, ensuring full control over processing, and the appropriate legal basis for further processing and how GDPR-compliant consent should be collected in cases of multiple processing.

In order to mitigate the risks to data subjects, the EDPB identifies three categories of personal data requiring special attention:

- Location data, which, due to its sensitive nature, should not be collected except if doing so is absolutely necessary for the purpose of processing;
- Biometric data, which should be stored locally and in encrypted form;
- Data revealing criminal offences and other infractions, the processing of which is subject to the safeguards contained in Art. 10 GDPR.

The EDPB also highlights the interplay between the GDPR and the ePrivacy Directive, noting that the connected vehicle and any device connected to it should be considered “terminal equipment” for the purposes of Art. 5(3) ePrivacy Directive.

Adopted: 28 January 2020

### **5.1.2. Guidelines 02/2020 on Arts. 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 its Guidelines, the EDPB provides guidance on the transfers of personal data from EEA public bodies to public bodies in third countries, or to international organisations, for the purpose of various administrative cooperation endeavours that fall within the scope of the GDPR.

The EDPB outlines general recommendations for additional appropriate safeguards to be adopted by public bodies for the transfer of personal data and notes the core data protection principles that are to be ensured by the parties to a transfer. Public bodies may implement appropriate safeguards either through a legally binding and enforceable instrument under Art. 46(2)(a) GDPR, or through provisions to be inserted into administrative arrangements under Art. 46(3)(b) GDPR.

The EDPB notes that any international agreement concluded between EEA and non-EEA public authorities should also safeguard data subject rights and provide for a redress mechanism that enables data subjects to exercise their rights in practice.

Adopted: 15 December 2020



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

*See Section 3.2.3 for a full summary.*

The GDPR's provisions on personal data processing for scientific research are also applicable in the context of the COVID-19 pandemic.

The EDPB Guidelines address key questions on the processing of health data for scientific research in the context of the pandemic.

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

*See Section 3.2.4 for a full summary.*

When processing personal data is necessary for implementing data-driven solutions in response to the COVID-19 pandemic, data protection is key to ensuring effective solutions, which are socially accepted. The EDPB clarifies the conditions and principles for the proportionate use of location data and contact-tracing apps.



### **5.1.5. Guidelines 05/2020 on consent under Regulation 2016/679**

Over the last decade, the Article 29 Working Party and the EDPB have issued guidance on consent as a legal basis for personal data processing. Past guidance has focused on defining valid consent as "freely given", "specific", "informed" and "unambiguous".

The EDPB updated the Article 29 Working Party guidance to avoid misinterpretation and to further clarify the meaning of consent with regard to personal data processing in the areas of cookie walls and user actions, such as scrolling or swiping. In this context, data controllers must ensure the following:

- Cookie walls must give users clear and equal options to accept or reject cookies;
- Cookie walls must allow users to access content without clicking "Accept Cookies". If content is inaccessible without making a choice about cookies, the user is not given a genuine choice and consent is therefore not "freely given";
- Actions such as scrolling or swiping through a webpage do not constitute a clear and affirmative action needed for lawful consent;
- Consent must be as easy to withdraw as it is to provide.

Adopted: 4 May 2020

### **5.1.6. Guidelines 06/2020 on the interplay with the Second Payments Services Directive and the GDPR**

The second Payments Services Directive (PSD2) repeals Directive 2007/64/EC and provides legal clarity for entities involved in the provision of payment services within the EEA.

The Guidelines are a more detailed and considered response, requested to support an initial letter, concerning regulatory

interplay between the GDPR and the PSD2. The Guidelines provide clarification on aspects related to the collection and processing of personal data by entities involved in the payments services sector. More specifically, the PSD2 provides clarity to those data controllers that have legal obligations associated with the PSD2. The EDPB confirms that controllers in the payment services sector should always ensure compliance with the requirements of the GDPR and stresses this importance. The EDPB, however, is appreciative of the regulatory uncertainty given the complexity of the interplay between the GDPR and the PSD2.

The Guidelines focus on a number of components critical to the interplay between the two legal frameworks. In summary, they provide guidance and clarity on the following subjects:

- Lawful grounds and further processing;
- Explicit consent;
- The processing of silent party data;
- The processing of special categories of data under the PSD2;
- Data minimisation, security, transparency, accountability and profiling.

Adopted: 17 July 2020

#### **5.1.7. Guidelines 07/2020 on the concepts of controller and processor in the GDPR**

This updated EDPB guidance builds upon and replaces the Article 29 Working Party Opinion 01/2010 (WP169) on the concepts of “controller” and “processor”, providing more developed and specific clarifications of these concepts in light of the changes brought by the GDPR.

The Guidelines offer a focus on definitions and pragmatic consequences attached to the different data protection roles, clarifying the following concepts:

- The concepts of controller, joint controller and processor are functional and autonomous concepts: they allocate responsibilities according to the actual roles of the parties and they should be interpreted mainly according to EU data protection law.
- The data controller may be defined by law or may be established on the basis of an assessment of the factual circumstances surrounding the processing. Controllers are the ones that determine both purposes and “means” of the processing, i.e. the “why” and the “how”;
- The data processor processes personal data on behalf of the controller and must not process the data other than according to the controller’s instructions, but the processor may be left a certain degree of discretion and may determine more practical aspects of the processing, including “non-essential means”. Data processing agreements between controllers and processors should include specific and concrete information on how the requirements set out by Art. 28 GDPR will be met;
- Joint controllers are two or more entities that jointly determine the purposes and means of the processing through “common decisions” or “converging decisions”, in such a manner that the processing by each party is inseparable. The distribution and allocation of obligations among joint controllers can have a degree of flexibility, as each controller shall ensure its processing is carried out in compliance with data protection requirements. Although the legal form of the arrangement among joint controllers is not specified by the GDPR, the EDPB recommends that it should be made in the form of a binding document.

Adopted: 2 September 2020

## 5.1.8. Guidelines 08/2020 on the targeting of social media users

As mechanisms used to target social media users become more sophisticated and an increasingly large number of data sources are combined and analysed for targeting purposes, the topic has gained increased public interest and regulatory scrutiny.

Within this environment, the EDPB identifies three key actors:

- Users: individuals who make use of social media;
- Social media providers: providers of an online service that enables the development of networks of users;
- Targeters: natural or legal persons that use social media services to direct specific messages to users.

Referring to relevant case law of the Court of Justice of the EU, such as the judgments in [Case C-40/17 \(Fashion ID\)](#), [Case C-25/17 \(Jehovah's Witnesses\)](#) and [Case C-210/16 \(Wirtschaftsakademie\)](#), the EDPB provides specific examples to clarify the roles of targeters and social media providers within different targeting mechanisms. Social media providers and targeters are often identified as joint controllers for the purposes of Art. 26 GDPR.

The EDPB also identifies the risks posed to the rights and freedoms of individuals as they result from processing personal data, including the possibility of discrimination and exclusion, and the potential for manipulating and influencing users. In this context, the EDPB highlights the relevant transparency requirements, the right of access and the joint controllers' duty to conduct a Data Protection Impact Assessment if the processing operations are "likely to result in a high risk" to the rights and freedoms of data subjects.

Adopted: 2 September 2020

## 5.1.9. Guidelines 09/2020 on relevant and reasoned objection under Regulation 2016/679

With increasing attention placed on the cooperation mechanism for SAs outlined in the GDPR, the EDPB guidance establishes a common understanding of the notion of a "relevant and reasoned" objection, on the basis of the definition enshrined in Art. 4(24) GDPR, and addresses its interpretation.

Under the cooperation mechanism, and specifically under Art. 60(3) GDPR, a Lead Supervisory Authority (LSA) is required to submit a draft decision to the Concerned Supervisory Authorities (CSAs), who may then raise a "relevant and reasoned objective" within the set timeframe.

In this context, the EDPB further clarifies the meaning of each of the elements of the definition in Art. 4(24) GDPR, which requires a relevant and reasoned objection to determine whether there is an infringement of the GDPR or whether the envisaged action in relation to the controller or processor complies with the GDPR, and 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 EU.

The EDPB notes that for an objection to be "relevant", there should be a direct connection between the draft decision at hand and the objection, since the objection, if followed, would entail a change to the draft decision leading to a different conclusion as to whether there is an infringement of the GDPR, or whether the envisaged action towards the controller or processor complies with the GDPR.

The objection will be "reasoned" when it is clear, precise, coherent and detailed in explaining the reasons for objection, through legal or factual arguments. The EDPB also provides clarifications on the obligation for the CSAs to clearly demonstrate in their objection the significance of the risks

posed by the draft decision for the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data.

Adopted: 8 October 2020

### **5.1.10. Guidelines 10/2020 on restrictions under Art. 23 GDPR**

The GDPR allows for data subject rights to be restricted in exceptional circumstances. The EDPB issued guidance on restrictions of data subject rights under Art. 23 GDPR. The Guidelines recall the conditions surrounding the use of such restrictions in light of the EU Charter of Fundamental Rights and the GDPR. They provide a thorough analysis of the criteria to apply restrictions, the assessments that must be observed, how data subjects can exercise their rights after the restrictions are lifted, and the consequences of infringing Art. 23 GDPR.

Under specific conditions, Art. 23 GDPR allows a national or EEA legislator to restrict, by way of a legislative measure, the scope of the rights and obligations enshrined in Chapter III GDPR (data subject rights) and corresponding provisions of Art. 5 GDPR, as well as Art. 34 GDPR, only if this restriction respects the essence of the relevant fundamental rights and freedoms, and is a necessary and proportionate measure in a democratic society to safeguard, amongst others, national security or important objectives of general public interest. The legislator issuing the legislative measures that set out the restrictions and the data controllers applying them should be aware of the exceptional nature of these restrictions.

The Guidelines provide details on the interpretation of each of these requirements, also highlighting how the requirement for a legislative measure can be met and the fact that such a measure needs to be adapted to the objective pursued. It also needs to meet the foreseeability criterion by being sufficiently clear so as to give individuals an adequate indication of the

circumstances in which controllers are empowered to resort to restrictions.

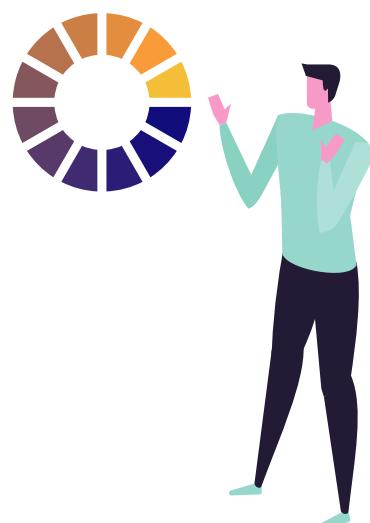
Restrictions under Art. 23 GDPR need to pass a necessity and proportionality test, typically implying the assessment of risks to the rights and freedoms of data subjects. The necessity test is based on the objective of general interest pursued. Only where the necessity test is satisfied, the proportionality of the measure is assessed.

The Guidelines also provide information concerning the specific requirements set out in Art. 23(2) GDPR, whereby the legislative measures setting out the restrictions need to contain specific provisions concerning a list of elements, including the purposes of processing, the scope of the restrictions, and the risks to the rights and freedoms of data subjects.

The controller should document the application of restrictions to concrete cases in line with the accountability principle and should lift the restrictions as soon as the circumstances that justify them no longer apply. Once restrictions are lifted, data subjects must be allowed to exercise all their rights in relation to the data controller.

SAs should be consulted before the adoption of the legislative measures setting the restrictions and have the powers to enforce compliance with the GDPR.

Adopted: 15 December 2020



### **5.1.11. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data supplementary measures**

*See Section 3.3.3 for the full summary.*

With these Recommendations, the EDPB seeks to help data exporters comply with EU law governing international transfers, as clarified by the Court of Justice of the EU in its judgment in Case C-311/18 (*Schrems II*). The Recommendations provide data exporters with six steps to follow to ensure that the personal data transferred is afforded a level of protection essentially equivalent to that guaranteed within the EU. The Recommendations also describe several examples of supplementary measures that could in certain situations contribute to ensuring the protection of personal data required under EU law.

### **5.1.12. Recommendations 02/2020 on the European Essential Guarantees for surveillance measures**

*See Section 3.3.4 for the full summary.*

These Recommendations update the content of a working document issued by the Article 29 Working Party with the clarifications that the Court of Justice of the EU and the European Court of Human Rights provided since the publication of this working document. The European Essential Guarantees describe four guarantees to be found when assessing the level of interference with the fundamental rights to privacy and data protection of surveillance measures in third countries.

### **5.1.13. Guidelines adopted following public consultation**

#### **5.1.13.1. Guidelines 03/2019 on processing personal data through video devices**

The proliferation of video devices in many spheres of individuals' daily lives has considerable implications for data protection and privacy. The use of facial recognition and analysis software could threaten to reinforce society's problematic prejudices, and systematic video surveillance could lead to an acceptance of the lack of privacy as the default.

In its Guidelines, the EDPB notes that the most likely legal bases for processing video surveillance data are legitimate interest under Art. 6(1)(f) GDPR and consent under Art. 6(1)(e) GDPR. When relying on legitimate interest as the legal basis, the necessity of deploying video surveillance needs to be proven, and a balancing test needs to be carried out on a case-by-case basis. When relying on consent, the EDPB recalls that it shall be "freely given, specific, informed and unambiguous".

The Guidelines highlight the need to pay particular attention to the processing of special categories of personal data, including biometric data. These could be identified when conducting a Data Protection Impact Assessment under Art. 35(1) GDPR, the results of which can inform the data protection measures that data controllers should implement.

The EDPB notes that the principle of transparency and the obligation to inform data subjects of video surveillance operations are crucial. The Guidelines elaborate on how controllers can fulfil these obligations and ensure that data subject rights can be exercised in practice.

Adopted: 29 January 2020

### **5.1.13.2. Guidelines 05/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1)**

The EDPB adopted the final version of its guidance with regards to the personal data processed by search engine providers and data subject requests for delisting.

The Guidelines provide insight into the six grounds on which to request delisting pursuant to Art. 17(1) GDPR, including when the personal data is no longer necessary in relation to its purposes, the data subject withdraws their consent, the personal data is otherwise unlawfully processed, or when the data subject exercises the right to object.

The EDPB also provided clarifications as to the exceptions to the right to request delisting as found in Art. 17(3) GDPR.

Adopted: 7 July 2020

### **5.1.13.3. Guidelines 04/2019 on Art. 25 GDPR Data Protection by Design and by Default Version 2.0**

Art. 25 GDPR enshrines the principles of Data Protection by Design and by Default (DPbDD), which form a crucial part of personal data protection legislation and act as key obligations for data controllers. Whilst the Guidelines mainly address data controllers, other actors such as processors and designers of products and services will also benefit from them.

The EDPB notes that controllers have to implement DPbDD through appropriate technical and organisational measures early on, and integrate necessary safeguards into the processing throughout its lifecycle. These measures ensure that data subject rights and freedoms are protected, and that data protection principles are effectively implemented.

The Guidelines also provide a number of recommendations for how controllers, processors and third parties in the ecosystem may cooperate to achieve DPbDD. In particular, they may engage Data Protection Officers from the outset, train employees on basic “cyber hygiene” and rely on codes of conduct to demonstrate compliance.

Adopted: 20 October 2020

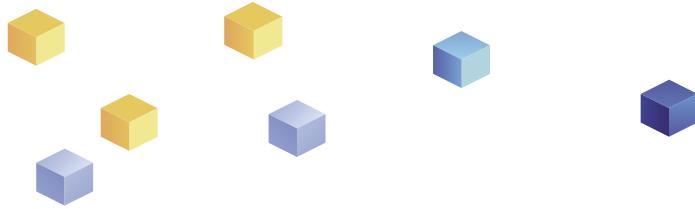
## **5.2. CONSISTENCY OPINIONS**

The EDPB aims to ensure the consistent application of the GDPR across the EEA. To enable this, SAs from EEA countries must request an Opinion from the EDPB before adopting any decision in areas specified by the GDPR as having cross-border implications. This applies when an SA does the following:

- Intends to adopt a list of the processing operations subject to the requirement for a Data Protection Impact Assessment;
- Intends to adopt a draft code of conduct relating to processing activities;
- Aims to approve the criteria for accreditation of certification bodies;
- Aims to adopt Standard Contractual Clauses;
- Aims to approve Binding Corporate Rules.

The competent SA must take utmost account of the Opinion. The EDPB’s Opinions pertaining to specific SAs and their implementation efforts are outlined below.

See Section 5.5.



### 5.2.1. Opinions on draft accreditation requirements for code of conduct monitoring bodies

The EDPB issued 11 Opinions on draft accreditation requirements for code of conduct monitoring bodies, as submitted by individual SAs. The SAs submitted their draft accreditation requirements and each requested an Opinion under Art. 64(1)(c) GDPR.

The aim of such EDPB Opinions is to ensure consistency and the correct application of the requirements among EEA SAs. In order to do so, the EDPB made several recommendations and encouragements to the various SAs on the amendments to be made to the draft accreditation requirements.

All SAs amended their drafts in accordance with Art. 64(7) GDPR, taking utmost account of the Opinions of the EDPB.

The various Opinions are listed below:

- Opinion 01/2020 on the Spanish data protection Supervisory Authority draft accreditation requirements for a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted: 28 January 2020
- Opinion 02/2020 on the Belgium data protection Supervisory Authority draft accreditation requirements for a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted: 28 January 2020
- Opinion 03/2020 on the France data protection Supervisory Authority draft accreditation requirements for a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted: 28 January 2020
- Opinion 10/2020 on the draft decision of the competent Supervisory Authorities of Germany regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted: 25 May 2020
- Opinion 11/2020 on the draft decision of the competent Supervisory Authority of Ireland regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted: 25 May 2020
- Opinion 12/2020 on the draft decision of the competent Supervisory Authority of Finland regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted: 25 May 2020
- Opinion 13/2020 on the draft decision of the competent Supervisory Authority of Italy regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted: 25 May 2020
- Opinion 18/2020 on the draft decision of the competent Supervisory Authority of the Netherlands regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted: 23 July 2020
- Opinion 19/2020 on the draft decision of the competent Supervisory Authority of Denmark regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted: 23 July 2020
- Opinion 20/2020 on the draft decision of the competent Supervisory Authority of Greece regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted: 23 July 2020
- Opinion 31/2020 on the draft decision of the competent Supervisory Authority of Poland regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted: 7 December 2020

## 5.2.2. Opinions on draft requirements for accreditation of a certification body

Ten SAs individually submitted their draft decisions on accreditation requirements for certification bodies under Art. 43(1)(b) GDPR to the EDPB, requesting an Opinion under Art. 64(1)(c) GDPR. The accreditation requirements allow the relevant national accreditation body to accredit certification bodies responsible for issuing and renewing certification in accordance with Art. 42 GDPR.

These Opinions aim to establish a consistent and harmonised approach regarding the requirements that SAs and national accreditation bodies apply when accrediting certification bodies under the GDPR. In order to do so, the EDPB made several recommendations and encouragements to the relevant SAs on the amendments to be made to the draft accreditation requirements.

The SAs then amended their drafts in accordance with Art. 64(7) GDPR, taking utmost account of the Opinions of the EDPB.

The various Opinions are listed below:

- Opinion 04/2020 on the draft decision of the competent Supervisory Authority of the United Kingdom regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43.3 GDPR Adopted: 29 January 2020
- Opinion 05/2020 on the draft decision of the competent Supervisory Authority of Luxembourg regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR Adopted: 29 January 2020
- Opinion 14/2020 on the draft decision of the competent Supervisory Authority of Ireland regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR Adopted: 25 May 2020

- Opinion 15/2020 on the draft decision of the competent Supervisory Authorities of Germany regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR Adopted: 25 May 2020
- Opinion 16/2020 on the draft decision of the competent Supervisory Authority of the Czech Republic regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR Adopted: 25 May 2020
- Opinion 21/2020 on the draft decision of the competent Supervisory Authority of the Netherlands regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR Adopted: 23 July 2020
- Opinion 22/2020 on the draft decision of the competent Supervisory Authority of Greece regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR Adopted: 23 July 2020
- Opinion 23/2020 on the draft decision of the competent Supervisory Authority of Italy regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR Adopted: 23 July 2020
- Opinion 26/2020 on the draft decision of the competent Supervisory Authority of Denmark regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43.3 (GDPR) Adopted: 7 December 2020
- Opinion 30/2020 on the draft decision of the competent Supervisory Authority of Austria regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43.3 (GDPR) Adopted: 7 December 2020

### 5.2.3. Opinions on draft decisions regarding Binding Corporate Rules

SAs may approve Binding Corporate Rules (BCRs) within the meaning of Art. 47 GDPR. BCRs are data protection policies implemented and adhered to within a group of enterprises established in the EEA for transfers of personal data outside the EEA within the same group.

In 2020, several SAs submitted their draft decisions regarding the Controller or Processor BCRs of various companies to the EDPB, requesting an Opinion under Art. 64(1)(f) GDPR. The EDPB issued nine Opinions on BCRs. In all instances, the EDPB concluded that the draft BCRs contained all required elements, and guaranteed appropriate safeguards to ensure that the level of protection in the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. They could therefore be adopted without changes.

The relevant SAs then went on to approve the BCRs.

The various Opinions are listed below:

- Opinion 06/2020 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of Fujikura Automotive Europe Group (FAE Group) Adopted: 29 January 2020
- Opinion 08/2020 on the draft decision of the Irish Supervisory Authority regarding the Controller Binding Corporate Rules of Reinsurance Group of America Adopted: 14 April 2020
- Opinion 09/2020 on the draft decision of the Irish Supervisory Authority regarding the Processor Binding Corporate Rules of Reinsurance Group of America Adopted: 14 April 2020
- Opinion 24/2020 on the draft decision of the Norwegian Supervisory Authority regarding the Controller Binding Corporate Rules of Jotun Adopted: 31 July 2020

- Opinion 25/2020 on the draft decision of the Swedish Supervisory Authority regarding the Controller Binding Corporate Rules of Tetra Pak Adopted: 31 July 2020
- Opinion 27/2020 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of Coloplast Group Adopted: 8 December 2020
- Opinion 28/2020 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of Iberdrola Group Adopted: 8 December 2020
- Opinion 29/2020 on the draft decision of the Lower Saxony Supervisory Authority regarding the Controller Binding Corporate Rules of Novelis Group Adopted: 8 December 2020
- Opinion 32/2020 on the draft decision of the Dutch Supervisory Authority regarding the Controller Binding Corporate Rules of Equinix Adopted: 15 December 2020

### 5.2.4. Other Opinions

Opinion 07/2020 on the draft list of the competent Supervisory Authority of France regarding the processing operations exempt from the requirement of a Data Protection Impact Assessment (Art. 35(5) GDPR) Adopted: 22 April 2020

Under Arts. 35(6) and 64(2) GDPR, the EDPB issues an Opinion where an SA intends to adopt a list of data processing operations not subject to the requirement for a Data Protection Impact Assessment pursuant to Art. 35(5) GDPR. The French Supervisory Authority (FR SA) submitted an update of its draft list of exempt processing activities to the EDPB for its consideration.

The EDPB clarified that 12 of the items included had already been considered in its Opinion on the previous version of the list submitted by the FR SA.

Similarly, for the thirteenth item, the EDPB referred to its previous Opinion, which addressed this kind of processing operation. For the remaining item, it was concluded that the draft list could lead to an inconsistent application of Art. 35 GDPR, so the EDPB recommended changes. Specifically, regarding the management of commercial activities, the FR SA was advised to restrict the scope of this item by covering only business-to-customers relations, and by excluding processing sensitive data or data of a highly personal nature from this item.

**Opinion 17/2020 on the draft Standard Contractual Clauses submitted by the SI SA (Art. 28(8) GDPR)** Adopted: 19 May 2020

The contract or other legal act to govern the relationship between the controller and the processor in accordance with Art. 28(3) GDPR may be based, in whole or in part, on Standard Contractual Clauses (SCCs). An SA may adopt SCCs in accordance with the consistency mechanism.

Therefore, the EDPB reviews draft SCCs submitted by SAs to contribute to the consistent application of the GDPR throughout the EU.

In February 2020, the Slovenian SA (SI SA) submitted its draft SCCs to the EDPB, requesting an Opinion under Art. 64(1)(d) GDPR. The EDPB made a number of recommendations on how to amend the draft SCCs. The EDPB also recalled that the possibility to use SCCs adopted by an SA does not prevent the parties from adding other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, the adopted SCCs or prejudice the fundamental rights or freedoms of the data subjects.

The SI SA amended its draft in accordance with Art. 64(7) GDPR, taking utmost account of the Opinion of the EDPB.

### 5.3. BINDING DECISIONS

**Decision 01/2020 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Twitter International Company under Article 65(1)(a) GDPR**

The EDPB adopted its first dispute resolution decision on the basis of Art. 65 GDPR. The binding decision addressed the dispute that arose after the Irish SA, acting as Lead Supervisory Authority (LSA), issued a draft decision regarding Twitter International Company (TIC) and the subsequent relevant and reasoned objections (RROs) expressed by a number of Concerned Supervisory Authorities (CSAs).

The LSA issued the draft decision based on its own investigation into TIC, after the company notified the LSA of a personal data breach on 8 January 2019.

In May 2020, the LSA shared its draft decision with the CSAs in accordance with Art. 60(3) GDPR. The CSAs then had four weeks to submit any RROs. Among others, the CSAs issued RROs on the infringements of the GDPR identified by the LSA, the role of TIC as the (sole) data controller and the calculation of the proposed fine. As the LSA rejected the objections and/or considered they were not “relevant and reasoned”, it referred the matter to the EDPB per Art. 60(4) GDPR, thereby initiating the dispute resolution procedure for the first time. The EDPB officially launched this procedure on 8 September 2020.





The EDPB's decision assessed whether each of the objections raised met the requirements set by Art. 4(24) GDPR. As a result, the main focus of the EDPB's decision was the compliance of the draft decision of the Irish SA with Art. 83 GDPR. Several SAs raised RROs that the proposed fine was insufficiently dissuasive.

With a view to the consistent application of the GDPR, the EDPB decided that the LSA was required to reassess the elements it relied upon to calculate the amount of the fine.

The LSA amended its draft decision by increasing the level of the fine to ensure it fulfilled its purpose as a corrective measure and met the requirements of effectiveness, dissuasiveness and proportionality established by Art. 83(1) GDPR, and taking into account the criteria of Art. 83(2) GDPR.

For further information see: [Art. 65 GDPR Frequently Asked Questions](#)

Adopted: 9 November 2020

## 5.4. CONSISTENCY PROCEDURES

The EDPB may produce documents to enable the consistent application of the GDPR across the EEA, as outlined here.

### 5.4.1. EDPB document on the procedure for the approval of certification criteria by the EDPB resulting in a common certification, the European Data Protection Seal

Arts. 42 and 43 GDPR introduce certification as a new accountability tool for data controllers and processors. Certification under Arts. 42 and 43 GDPR can be issued for processing operations by controllers and processors.

Certification under the GDPR shall be issued by accredited certification bodies or by the competent SAs, on the basis of criteria approved by that competent SA or by the EDPB. In this regard, Art. 43(5) GDPR refers to the approval of certification criteria with an EU-wide reach, namely, the European Data Protection Seal.

The EDPB document develops the procedure for the approval of a European Data Protection Seal, focusing on harmonisation and consistency. The approval procedure consists of two phases: an informal cooperation phase and the formal approval phase.

The informal cooperation phase involves all SAs and includes a review of the technical issues linked to the certification criteria, and a national legislation compatibility check. If substantial issues are identified, they can be brought to the relevant EDPB expert subgroup for discussion.

The procedure also foresees the possibility for the scheme owner to ask for clarifications and respond to comments made during the informal phase.

The formal approval phase is based on the procedure for requesting an Art. 64(2) GDPR Opinion. Therefore, the SA submitting the criteria for an Opinion of the EDPB has to provide written reasoning for the request. In this context, the document notes that the SA has to ask for an Opinion under Art. 64(2) GDPR regarding a matter producing effects in more than one Member State. The EDPB Secretariat will then be in charge of drafting the Opinions and, upon decision of the Chair, together with a rapporteur and expert subgroup members.

The EDPB's approval process is completed by the adoption of an Opinion approving or rejecting the EU Data Protection Seal request for the submitted criteria. The EDPB's Opinion is applicable in all Member States.

Adopted: 28 January 2020

#### **5.4.2. EDPB document on the procedure for the development of informal “Codes of Conduct sessions”**

The EDPB document develops the procedure for the approval of transnational codes of conduct, focusing on harmonisation and consistency. The approval procedure consists of two phases: an informal cooperation phase and the formal approval phase. The procedures build on Guidelines 01/2019 on Codes of Conduct and, in particular, its Section 8.

The informal cooperation phase involves all SAs and the “Code sessions” are presented as a forum for informal discussions on transnational Codes of Conduct that have not yet been formally submitted to the EDPB, with the aim of finding a consensus on the standards and expectations for Codes of Conduct and making these clear to the code owners. If there is a need for agreements regarding substantial elements of the Codes of Conduct, they can be brought to the relevant EDPB expert subgroup for discussion.

The document further clarifies the nature and format of the Code sessions and elaborates on the role of SAs, and their interaction with both the Competent SAs and the Code owners, as well as on the role of the EDPB Secretariat and the different phases of the approval process.

The formal approval phase is based on the procedure for requesting an Art. 64(1) GDPR Opinion. The EDPB Secretariat, together with two co-rapporteurs, is in charge of drafting the Opinions.

Adopted: 10 November 2020

#### **5.5. REGISTER FOR DECISIONS TAKEN BY SUPERVISORY AUTHORITIES AND COURTS ON ISSUES HANDLED IN THE CONSISTENCY MECHANISM**

One of the roles of the EDPB is to maintain a publicly accessible electronic [register of decisions](#) taken by SAs and courts on issues handled in the consistency mechanism per Art. 70(1) (y) GDPR. This section outlines key decisions taken by various SAs, particularly in response to EDPB Opinions on the topic of their actions.

See Section 5.2.

##### **5.5.1. Approval of Binding Corporate Rules of Fujikura Automotive Europe Group (FAE Group)**

As the BCR Lead Supervisory Authority (LSA) in this case, the Spanish SA communicated a draft decision on the Controller BCRs of Fujikura Automotive Europe Group (FAE Group) to the EDPB in accordance with Art. 64(1)(f) GDPR.

The EDPB provided its [Opinion 6/2020](#) (January 2020) on the SA's draft decision. The SA took utmost account of that Opinion and adopted its final decision approving the Controller BCRs of FAE Group in accordance with Art. 47(1) GDPR, finding that the BCRs provide appropriate safeguards for the transfer of personal data to members of the FAE Group established in third countries.

Adopted: 11 March 2020



## **5.5.2. Decision of the Irish Supervisory Authority approving the Controller Binding Corporate Rules of RGA International Reinsurance Company DAC (RGAI)**

As the BCR LSA in this case, the Irish SA communicated a draft decision on the Controller BCRs of RGA International Reinsurance Company DAC (RGAI) to the EDPB in accordance with Art. 64(1)(f) GDPR.

The EDPB provided its [Opinion 08/2020](#) (April 2020) on the SA's draft decision. The SA took utmost account of that Opinion and adopted its final decision approving the Controller BCRs of RGAI in accordance with Art. 47(1) GDPR, finding that the BCRs provide appropriate safeguards for the transfer of personal data to members of the RGAI Group established in third countries.

Adopted: 1 May 2020

## **5.5.3. Decision of the Irish Supervisory Authority approving the Processor Binding Corporate Rules of RGA International Reinsurance Company DAC (RGAI)**

As the BCR LSA in this case, the Irish SA communicated a draft decision on the Processor BCRs of RGA International Reinsurance Group DAC (RGAI) to the EDPB in accordance with Art. 64(1)(f) GDPR.

The EDPB provided its [Opinion 09/2020](#) (April 2020) on the SA's draft decision. The SA took utmost account of that Opinion and adopted its final decision approving the Processor BCRs of RGAI in accordance with Art. 47(1) GDPR, finding that they provide appropriate safeguards for the transfer of personal data to members of the RGAI Group established in third countries.

In its review of the Processor BCRs, the SA concluded that they comply with the requirements set out by Arts. 47(1) and 47(2) GDPR and contain clear responsibilities with regards to personal data processing.

Adopted: 1 May 2020

## **5.5.4. Decision of the Slovakian Supervisory Authority authorising the Administrative Arrangement for the transfer of personal data between EEA Financial Supervisory Authorities and non-EEA Financial Supervisory Authorities**

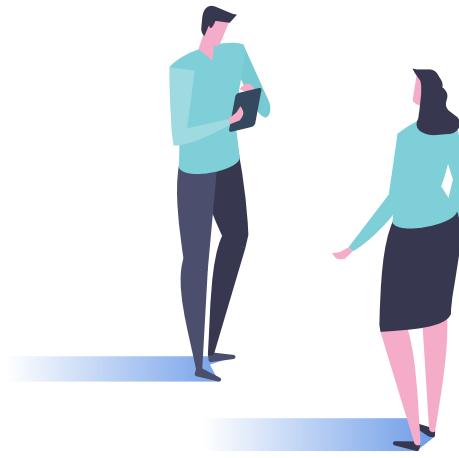
Following the EDPB's [Opinion 04/2019](#), the Slovakian SA authorised the Administrative Arrangement for the transfer of personal data between EEA Financial Supervisory Authorities and non-EEA Financial Supervisory Authorities.

In its decision, the SA noted that the provisions contained in the Administrative Arrangement provide appropriate safeguards for the transfer of personal data between EEA Financial Supervisory Authorities and non-EEA Financial Supervisory Authorities, in accordance with Art. 46(3)(b) GDPR.

The SA will monitor the practical application of the Administrative Arrangement, particularly in relation to data subject rights, onward transfers, redress and oversight mechanisms.

Adopted: 4 May 2020





### **5.5.5. Irish Supervisory Authority's additional accreditation requirements for certification bodies**

The Irish SA adopted the additional accreditation requirements for certification bodies with respect to ISO/IEC 17065/2012 (ISO 17065) and per Arts. 43(1) and 43(3) GDPR. The document contains the requirements necessary to assess the competence, consistent operation and impartiality of certification bodies that intend to issue certifications pursuant to Arts. 42 and 43 GDPR.

As underlined in the requirements, certification under the GDPR is only applicable to processing operations of controllers and processors. In order to issue GDPR certifications, certification bodies must be accredited in accordance with the requirements adopted by the competent SA.

The approval of the additional accreditation requirements by the Irish SA will allow certification bodies that want to issue GDPR certification to apply for accreditation.

Adopted: 1 June 2020

### **5.5.6. Decision of the Swedish Supervisory Authority approving the Binding Corporate Rules of Tetra Pak Group**

As the BCR LSA in this case, the Swedish SA adopted a decision to approve the Controller BCRs of Tetra Pak Group following the EDPB's Opinion 25/2020 (July 2020) on its draft decision.

The SA took utmost account of that Opinion and adopted its final decision approving the Controller BCRs of Tetra Pak Group in accordance with Art. 47(1) GDPR, finding that they provide appropriate safeguards for the transfer of personal data to members of Tetra Pak Group established in third countries.

Adopted: 17 August 2020

### **5.5.7. Decision of the Norwegian Supervisory Authority approving the Binding Corporate Rules of Jotun Group**

As the BCR LSA in this case, the Norwegian SA adopted a decision to approve the Controller BCRs of Jotun to the EDPB following the EDPB's Opinion 24/2020 (July 2020) on its draft decision.

The SA took utmost account of that Opinion and adopted its final decision approving the Controller BCRs of Jotun in accordance with Art. 47(1) GDPR, finding that they provide appropriate safeguards for the transfer of personal data to members of the Jotun Group established in third countries.

Adopted: 18 August 2020

### **5.5.8. German Supervisory Authorities' requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR**

The German SAs amended their requirements for accreditation of a certification body based on Art. 43(3) GDPR in connection with Art. 57(1)(p) GDPR.

The revised requirements are a response to the EDPB's Opinion 15/2020 on the German SAs' draft decision.

The document contains the requirements necessary to assess the competence, consistent operation and impartiality of certification bodies that intend to issue certifications pursuant to Arts. 42 and 43 GDPR. The bodies that want to issue GDPR certification may then apply for accreditation.

As the requirements state, certification under the GDPR is only applicable to processing operations of controllers and processors. Certification bodies must be accredited in accordance with the requirements adopted by the competent SA in order to issue GDPR certifications.

Adopted: 8 October 2020

### **5.5.9. German Supervisory Authorities' accreditation requirements for a GDPR code of conduct monitoring body pursuant to Art. 41(3) GDPR**

The German SAs amended the requirements applicable in Germany for the accreditation of a GDPR code of conduct monitoring body in response to EDPB Opinion 10/2020 on their draft decision. The SAs outlined the administrative and substantive requirements to be fulfilled by the code of conduct monitoring body to receive accreditation.

Approval of the accreditation requirements by the German SAs will allow monitoring bodies to apply for the necessary accreditation in relation to specific GDPR codes of conduct.

Adopted: 8 October 2020

### **5.5.10. Irish Supervisory Authority's accreditation requirements for a GDPR code of conduct monitoring body pursuant to Art. 41(3) GDPR**

The Irish SA adopted the accreditation requirements of a code of conduct monitoring body following the EDPB's Opinion 11/2020 on its draft. In its decision, the SA outlined the administrative and substantive requirements to be fulfilled by the monitoring body to receive accreditation. The requirements include explanatory notes and examples in order to further elaborate on specific requirements or list some elements that may be provided to demonstrate compliance with the requirements.

As established in the GDPR, and underlined in the requirements, the monitoring of compliance with a code of conduct is carried out by accredited monitoring bodies. As such, monitoring bodies are accredited to monitor a specific code of conduct and, therefore, the compliance with the requirements for accreditation has to be demonstrated in relation to a specific code of conduct.

The approval of the accreditation requirements by the Irish SA will allow monitoring bodies to apply for the necessary accreditation in relation to specific codes of conduct.

Adopted: 9 October 2020

### **5.5.11. Danish Supervisory Authority's accreditation requirements for a GDPR code of conduct monitoring body pursuant to Art. 41(3) GDPR**

The Danish SA adopted the requirements applicable in Denmark for the accreditation of code of conduct monitoring bodies following EDPB Opinion 19/2020 on its draft decision.

In its decision, the SA outlined the administrative and substantive requirements to be fulfilled by the monitoring body to receive accreditation.

Monitoring bodies are accredited to monitor a specific code of conduct and, therefore, the compliance with the requirements for accreditation has to be demonstrated in relation to a specific code of conduct.

The approval of the accreditation requirements by the Danish SA will allow monitoring bodies to apply for the necessary accreditation in relation to specific codes of conduct.

Adopted: 12 November 2020

#### **5.5.12. Decision under S.111 of the Irish Data Protection Act 2018 and for the purposes of Art. 60 GDPR in the matter of Twitter International Company**

The Irish SA submitted the case of Twitter International Company (TIC) to the consistency mechanism referred to in Art. 63 GDPR as a result of objections raised by other SAs in respect to the Irish SA's draft decision in the case at hand.

The Irish SA began an inquiry on 22 January 2019 to examine whether TIC complied with its obligations to notify the SA of a personal data breach per Art. 33(1) GDPR, and whether TIC adequately documented the breach as per Art. 33(5) GDPR. The final decision was issued on 9 December 2020, in line with Art. 65(6) GDPR, which requires the addressee of an EDPB decision taken on the basis of Art. 65 GDPR to adopt its final decision within one month of the notification of the EDPB decision.

- The Irish SA found that TIC did not comply with its obligations in Arts. 33(1) and 33(5) GDPR and elaborated upon the reasons for this conclusion. In assessing the administrative fine to be imposed as a result, the SA

referred to EDPB [Decision 01/2020](#), which requested that the SA reassess the elements upon which the fine is to be determined, and considers the criteria outlined by Art. 83(2) GDPR.

In the matter of TIC's compliance with the requirements found in Arts. 33(1) and 33(5) GDPR, the Irish SA decided to impose an administrative fine of USD 500,000 (EUR 450,000).

Adopted: 9 December 2020

### **5.6. LEGISLATIVE CONSULTATION**

#### **5.6.1. EDPB Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic**

*See Section 3.2.2 for a full summary.*

In its draft Guidance on apps supporting the fight against the COVID-19 pandemic, the European Commission proposed the development of a pan-European and coordinated approach in the use of such tools. The EDPB welcomes this initiative and addresses specifically the use of apps for contact-tracing and warning individuals.

#### **5.6.2. Statement on the ePrivacy Regulation and the future role of Supervisory Authorities and the EDPB**

The EDPB adopted its Statement with regards to the role of SAs and the EDPB in the context of the [ePrivacy Regulation](#) currently being negotiated. The EDPB highlights the importance of avoiding the fragmentation of supervision, procedural complexity and diverging interpretations through the enforcement of the future ePrivacy Regulation.

In this context, the EDPB underlines that many of the provisions of the future ePrivacy Regulation relate to the processing of personal data and are intertwined with provisions of the GDPR. Thereby the oversight of the ePrivacy Regulation should be entrusted to the same national authorities, which are responsible for enforcement of the GDPR. Further, the EDPB notes that the existing cooperation and consistency mechanism for the supervision and enforcement of the GDPR should also be adopted for the supervision of the ePrivacy Regulation in the context of personal data processing and would lead to more harmonisation and consistency. The same framework would also benefit data controllers through a single point of contact and guarantee a level playing field on the EU Digital Single Market.

Adopted: 19 November 2020

## 5.7. OTHER DOCUMENTS

### 5.7.1. Contribution of the EDPB to the evaluation of the GDPR

*See Section 3.1 for a full summary.*

The EDPB and national SAs contributed to the European Commission's evaluation and review of the GDPR, as required by Art. 97 GDPR. The EDPB considers that the GDPR has strengthened data protection as a fundamental right and harmonised the interpretation of data protection principles, and believes it is premature to revise it at this point in time.

### 5.7.2. Statement on privacy implications of mergers

The EDPB adopted a statement on privacy implications of mergers having noted the intention of Google LLC to acquire Fitbit, Inc. The EDPB expressed concerns regarding the

potentially high level of risk to the fundamental rights to privacy and personal data entailed by the possible further combination and accumulation of sensitive personal data by a major tech company. The EDPB reminded the parties of their obligations under the GDPR and of the need to conduct in a transparent way a full assessment of the data protection requirements and privacy implications of the merger. The EDPB expressed its readiness to contribute further advice on the proposed merger to the European Commission if so requested.

Adopted: 19 February 2020

### 5.7.3. Statement on the processing of personal data in the context of the COVID-19 outbreak

*See Section 3.2.1 for a full summary.*

The EDPB emphasises that respecting data protection rules does not hinder the response to the COVID-19 pandemic. Even in exceptional times, data controllers and processors must ensure the protection of personal data.

Adopted: 19 March 2020

### 5.7.4. Statement on restrictions on data subject rights in connection to the state of emergency in Member States

*See Section 3.2.5 for a full summary.*

The EDPB emphasises that when EEA Member States enter a state of emergency, such as that brought on by the COVID-19 outbreak, the GDPR remains applicable and allows for efficient emergency response while protecting fundamental rights and freedoms.

Adopted: 2 June 2020

### **5.7.5. Statement on the processing of personal data in the context of reopening of borders following the COVID-19 outbreak**

*See Section 3.2.6 for a full summary.*

The EDPB urges EEA Member States to adopt a standardised approach to the processing of personal data in the context of reopening borders during the COVID-19 pandemic and emphasises that data processing must be necessary and proportionate.

Adopted: 16 June 2020

### **5.7.6. Statement on the data protection impact of the interoperability of contact tracing apps**

*See Section 3.2.7 for a full summary.*

The EDPB maintains that, without a common EEA approach in response to the COVID-19 pandemic, an interoperable framework should be put in place regarding contact tracing apps and then outlines seven key focus areas.

Adopted: 16 June 2020

### **5.7.7. Statement on the Court of Justice of the European Union Judgment in Case C-311/18 – Data Protection Commissioner v Facebook Ireland and Maximillian Schrems**

*See Section 3.3.1 for a full summary.*

The EDPB believes that the CJEU's judgment in Case C-311/18 (*Schrems II*) highlights the importance of the fundamental right to privacy in the context of the transfer of personal data to third countries, and the risk for data subjects caused by possible

indiscriminate access by a third country's public authorities to the personal data transferred. Standard Contractual Clauses that enable data transfers must maintain a level of protection in the third country that is essentially equivalent to that in the EEA.

Adopted: 17 July 2020

### **5.7.8. Information note on BCRs for Groups of undertakings / enterprises which have ICO as BCR Lead SA**

The EDPB issued an information note with regards to arrangements for enterprises that have BCRs where the UK SA is the competent SA. In light of Brexit, such BCR holders need to make all organisational arrangements to establish a new BCR Lead SA in the EEA.

The EDPB notes that any current BCR applications before the UK SA are also encouraged to put in place organisational arrangements on the basis of which a new BCR Lead SA in the EEA can be established. This should be completed before the end of the Brexit transition period.

With the aim of providing clarification to BCR holders, the EDPB has a practical checklist of elements that must be amended to ensure their BCRs remain a valid transfer mechanism for transfers of data outside the EEA after the transition period. The same checklist informs applicants with BCRs undergoing review by the UK SA as to which changes need to become effective (at the latest) at the end of the transition period.

Adopted: 22 July 2020



### **5.7.9. Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 – Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems**

See Section 3.3.1 for a full summary.

Following the CJEU's judgment in Case C-311/18 (*Schrems II*), the EDPB provided clarifications on the judgment in a document addressing 12 Frequently Asked Questions (FAQs) about personal data transfers from the EEA to the U.S. and other third countries.

Adopted: 23 July 2020

### **5.7.10. EDPB Document on Coordinated Enforcement Framework under Regulation 2016/679**

In this Document, the EDPB introduces the Coordinated Enforcement Framework (CEF), which builds upon and supports mechanisms for cooperation as outlined in the GDPR.

In this context, the CEF provides a structure for annual coordinated actions by EDPB SAs. The objective of the CEF is to facilitate joint actions, such as joint awareness-raising activities, information gathering and joint investigations. Coordinated actions thus contribute to GDPR compliance, the protection of the rights and freedoms of citizens, and to reducing the risks of new technologies to the right of personal data protection.

In this Document, the EDPB provides an illustrative overview of the structure of the CEF and outlines its lifecycle, stipulates its legal basis and the division of competences between the EDPB and the SAs, as well as indicating the relationship between the CEF and the cooperation and consistency mechanism under the GDPR.

Adopted: 20 October 2020

### **5.7.11. Statement on the protection of personal data processed in relation with the prevention of money laundering and terrorism financing**

The EDPB adopted its Statement following the launch of the public consultation in May 2020 on the European Commission's Action Plan for a comprehensive Union policy for the prevention of money laundering and terrorist financing for a comprehensive Union policy for the prevention of money laundering and terrorist financing. In its Statement, the EDPB reaffirms the existing interplay between the protection of privacy, personal data and anti-money laundering measures, and stresses the need to address this relationship in the updated legislation.

Specifically, the relevance and accuracy of the data collected plays a paramount role, as well as the need to specify a clear legal basis, and define the limits and purposes of personal data processing. The EDPB notes that this is especially pertinent in the context of international data transfers and information sharing, as has also been noted by the EDPS in his Opinion on the same Action Plan.

The EDPB highlights the importance of the compatibility of the anti-money laundering measures with the rights to privacy and data protection, as enshrined in the EU Charter of Fundamental Rights, and the principles of necessity and proportionality.

Adopted: 15 December 2020



## **5.7.12. EDPB Document on Terms of Reference of the EDPB Support Pool of Experts**

Within its mission of ensuring a high and consistent level of protection of personal data throughout the EEA Member States, and as part of its investigatory and enforcement activities, the EDPB adopted the Terms of Reference of its Support Pool of Experts (SPE), which aims to provide material support to EDPB Members and to enhance cooperation and solidarity between all EDPB Members. The SPE comprises both EDPB experts and external experts, and is deployed to assist the carrying out of support investigations and enforcement activities of significant common interest.

The EDPB Document outlines the different types of support activities that the SPE may provide, including analytical support, the preparation of investigative reports and assisting in the performance of findings of a forensic nature. The EDPB notes the legal bases for the creation of the SPE, which are outlined in the GDPR, and elaborates on the key principles of SPE involvement, including the principles of voluntariness, confidentiality and coordination. In its Document, the EDPB also outlines the composition of the SPE, the role of the EDPB and external experts involved therein, as well as the process of reporting and evaluation.

Adopted: 15 December 2020

## **5.7.13. Pre-GDPR Binding Corporate Rules overview list**

The EDPB published a list of pre-GDPR BCRs on its website. This list provides information on BCRs that were submitted to SAs in accordance with the rules applicable under Directive 95/46 and for which the procedure for approval ended prior to 25 May 2018, when the GDPR started applying. The list notes 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.

Adopted: 21 December 2020 (updated on 26 January 2021)

## **5.7.14. Information note on data transfers under the GDPR to the United Kingdom after the transition period**

The first version of the note, adopted on 15 December 2020, described the situation in which transfers of personal data to the UK constitute transfers to a third country. However, the document was updated taking into consideration that on 24 December 2020, an agreement was reached between the EU and the UK. The agreement provides that for a maximum period of six months from its entry into force – i.e., until 30 June 2021 at the latest - and upon the condition that the UK's current data protection regime stays in place, all flows of personal data between stakeholders subject to the GDPR and UK organisations will not be considered as such international transfers.

Until 30 June 2021, at the latest, organisations subject to the GDPR will be able to carry on transferring personal data to UK organisations without the need to either put in place a transfer tool under Art. 46 GDPR or rely on an Art. 49 GDPR derogation. If no adequacy decision applicable to the UK as per Art. 45 GDPR is adopted by 30 June 2021 at the latest, all transfers of personal data between stakeholders subject to the GDPR and UK entities will then constitute a transfer of personal data to a third country.

The EDPB recalls the specific [information note](#) it has previously issued on the topic, as well as the specific guidance on possible supplementary measures in its [Recommendations 01/2020](#).

Adopted: 15 December 2020 (updated on 13 January 2021)

### **5.7.15. Statement on the end of the Brexit transition period**

The first version of the Statement, adopted on 15 December 2020, was updated taking into consideration that on 24 December 2020, an agreement on future relations was reached between the EU and the UK. The EDPB reminds all stakeholders that the 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 the GDPR and UK entities will not be considered as transfers to a third country subject to the provisions of Chapter V GDPR. This interim provision applies for a maximum period of six months (i.e., until 30 June 2021 at the latest).

The EDPB specifies that, as of 1 January 2021, the One-Stop-Shop (OSS) mechanism is no longer applicable to the UK, so the UK Information Commissioner's Office is no longer part of it.

The EDPB wishes to emphasise that the decision to benefit from the unified dialogue enabled by the OSS mechanism in cross-border processing cases is up to the individual controllers and processors, who to that end may decide whether to set up a new main establishment in the EEA under the terms of Art. 4(16) GDPR.

The EDPB recalls that controllers and processors not established in the EEA, but whose processing activities are subject to the application of the GDPR under Art. 3(2) GDPR, are required to designate a representative in the Union in accordance with Art. 27 GDPR.

Adopted: 15 December 2020 ([updated](#) on 13 January 2021)

### **5.8. PLENARY MEETINGS AND EXPERT SUBGROUPS**

Between 1 January and 31 December 2020, the EDPB held 27 plenary meetings. The [agendas](#) and [minutes](#) of the plenary sessions are published on the EDPB website. During these meetings, the EDPB adopted Guidelines, Opinions and other documents such as statements or information notes to advise the European Commission, national SAs and other stakeholders on GDPR matters, as outlined earlier in this chapter. In addition, there were 145 expert group meetings. In total, 268 meetings were held, including plenary meetings, expert subgroup meetings and drafting team meetings.

The different expert subgroups focus on specific areas of data protection and assist the EDPB in performing its tasks. Chapter 9 outlines the list of the expert subgroups and their respective mandates.

### **5.9. STAKEHOLDER CONSULTATION AND TRANSPARENCY**

#### **5.9.1. Stakeholder events on future guidance**

The EDPB organises stakeholder events to gather input and views on specific issues in the interest of developing future guidance. In 2020, the EDPB organised one such event on legitimate interest. This event was held entirely online due to the COVID-19 pandemic. Participants gave examples of how they had been using legitimate interest as a legal basis for data processing, and highlighted areas that needed clarifying or explaining. The EDPB will use this stakeholder input in the context of drafting future guidance on legitimate interest.

## 5.9.2. Public consultations on draft guidance

Following the preliminary adoption of Guidelines, the EDPB organises public consultations to give stakeholders and citizens the opportunity to provide additional input. The EDPB Members in charge of drafting the Guidelines consider this input in the subsequent drafting process. The Guidelines are then adopted in their final version.

To further enhance transparency, the EDPB publishes on its website stakeholders' contributions to public consultations. In 2020, the EDPB launched several such consultations:

- In February, the EDPB opened public consultations on both Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications and Guidelines 02/2020 on Arts. 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. It received 62 contributions to the Guidelines 01/2020 on connected vehicles, including input from U.S.-based business organisations. Guidelines 02/2020 received contributions from 12 entities, mainly comprising public authorities.
- In July, Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR were opened for public consultation. The EDPB received 39 contributions.
- The EDPB published Guidelines 07/2020 on the concepts of controller and processor in the GDPR and Guidelines 08/2020 on the targeting of social media users for consultation in September. 109 entities gave input on Guidelines 07/2020 on controllers and processors, and 33 gave input on Guidelines 08/2020 on targeting social media users.
- In October, Guidelines 09/2020 on relevant and reasoned objection under Regulation 2016/679 were opened for public consultation and received three contributions.

- In December, the EDPB launched public consultations on Guidelines 10/2020 on restrictions under Art. 23 GDPR, which received 11 contributions.
- Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data were open for public input in November. 193 entities, comprising mainly business associations, submitted responses.

## 5.9.3. Stakeholder survey on adopted guidance

For the third year in a row, the EDPB conducted a survey as part of the annual review of the EDPB's activities under Art. 71(2) GDPR. Questions centred on the EDPB's work and output in 2020, with a focus on its Guidelines and Recommendations, all with a view to understanding the extent to which stakeholders find the EDPB's guidance helpful in interpreting the GDPR's provisions, and in order to identify future paths to better support organisations as they approach data protection.

### 5.9.3.1. Participants

Multiple entities, including individual companies and Non-Governmental Organisations, representing different countries, sectors and business sizes, participated in the survey. Businesses and other private organisations were most represented.

### 5.9.3.2. Findings

In line with the results of the 2019 survey, most stakeholders participating in the 2020 survey found the Guidelines and Recommendations to be helpful in interpreting the GDPR and/or to provide actionable guidance for their activities. The most positive feedback applied to Guidelines 01/2020, 02/2020,

03/2020, 09/2020, 10/2020 and the Recommendation 02/2020. The second most mentioned comment was that, although the Guidelines contained useful and actionable information, they did not answer all the questions of the respondent. This applied in particular to Guidelines 02/2020 and 08/2020. The EDPB's guidance on the concepts of controller and processor, measures to supplement data transfer tools, and consent were notably popular. However, stakeholders considered the Recommendations 02/2020 as not helpful or clear enough. The results showed that participants had consulted, on average, five Guidelines and Recommendations.

Stakeholders were satisfied with the examples used in the EDPB Guidelines and some expressed a desire for further examples, for example with regard to the targeting of social media users. The addition of an executive summary to more Guidelines was well received and respondents would like to see it as a standard section of guidance documents. More often than not, the EDPB guidance triggered a change in the broader strategy of the respondent organisations.

A majority of respondents had participated in at least one EDPB workshop and most who had done so found the overall experience positive. Participants appreciated the useful and insightful information shared by the EDPB during the workshops, especially as they created room for interaction. Similarly, most respondents had participated in the consultation process for certain Guidelines and found the experience positive. Having the possibility to raise concerns created a welcome form of dialogue. Some respondents expressed a desire for more meetings with the relevant stakeholders to enable more input.

Stakeholders mostly found the relevant Guidelines and Recommendations directly on the EDPB website.

### 5.9.3.3. Conclusions

The EDPB highly appreciated the stakeholders' participation and useful contribution to the EDPB's work. Feedback on the guidance's operational value and alignment with other EU laws was equally appreciated as it gave actionable insights into stakeholder needs. The EDPB also welcomed stakeholders' value of transparency and interest in participating in the adoption process. In 2021, the EDPB is committed to continuing its cooperation and outreach to inform the development and effectiveness of future guidance.

### 5.9.4. Transparency and access to documents

Transparency is a core principle of the EDPB. As an EU body, the EDPB is subject to Art. 15 of the [Treaty of the Functioning of the European Union](#) and to [Regulation 1049/2001 on public access to documents](#). Art. 76(2) GDPR and Art. 32 of the EDPB's Rules of Procedure reinforce this requirement. Upholding the principle of transparency means that any citizen of the EU, and any natural or legal person residing or having its registered office in a Member State, has the right of access to EDPB documents. This right applies to all documents held by the EDPB, concerning any matter relating to its responsibilities. In exceptional cases, the EDPB may refuse to disclose all or part of a document. The reasons for refusal and other procedural rules are outlined in [Regulation 1049/2001 on public access to documents](#).

In 2020, there were 42 public access requests registered for documents held by the EDPB.

## 5.10. EXTERNAL REPRESENTATION OF THE EDPB

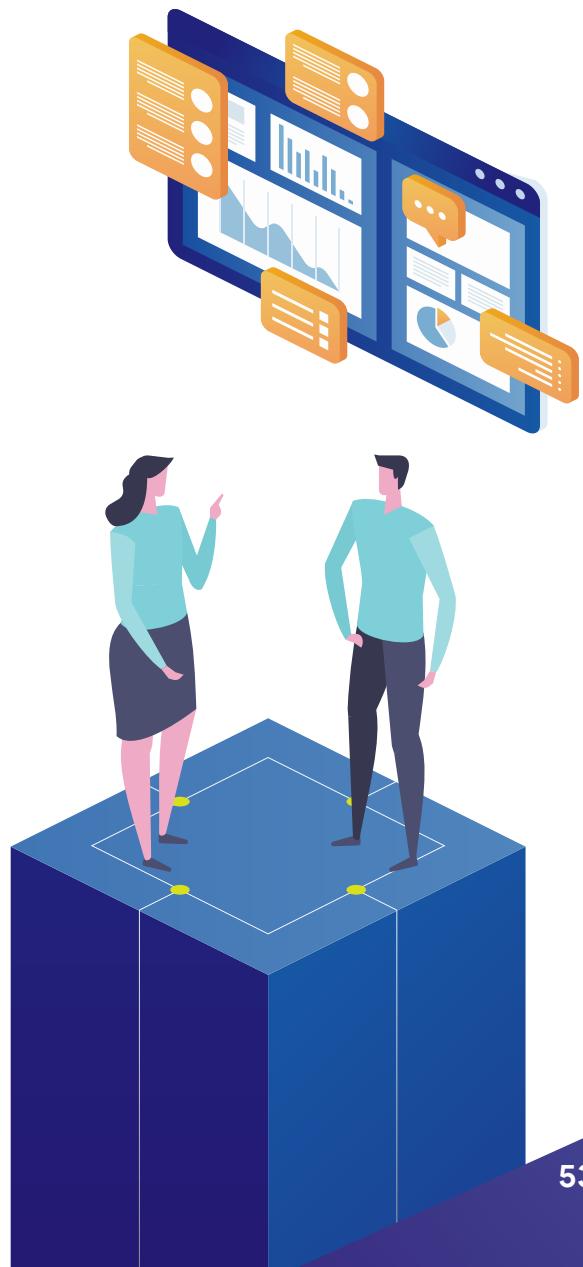
Public awareness and cooperation are vital to upholding data protection rights in the EEA and beyond, which is why the EDPB values stakeholder and citizen engagement. The EDPB Secretariat supports the Chair and Deputy Chairs in engagements with other EU institutions or bodies, and when they represent the EDPB at conferences and multi-stakeholder platforms. Staff members from the EDPB Secretariat also take part in several events to present the activities of the EDPB.

### 5.10.1. Participation of Chair and Deputy Chairs in conferences and speaking engagements

In 2020, the Chair of the EDPB, Andrea Jelinek, had over 20 speaking engagements, despite many events being cancelled or postponed due to the COVID-19 pandemic. She gave almost all presentations remotely. The speaking engagements included press briefings, presentations and panel debates for a range of institutes, academic forums and policy agencies. The Chair also met with European Commissioners and representatives from, amongst others, the Committee on Civil Liberties, Justice and Home Affairs Committee of the European Parliament. The Chair engaged with stakeholders beyond the EU. The EDPB Deputy Chair Ventsislav Karadjov took part in four speaking engagements, including speeches and panel presentations.

### 5.10.2. Participation of EDPB Staff in conferences and speaking engagements

EDPB staff represented the EDPB at a number of events, both in-person and remotely. The events were hosted by, amongst others, universities and trade associations. EU representatives discussed timely issues, such as data protection in the age of the COVID-19 pandemic as well as international data transfers after the *Schrems II* decision.



# 6



## Supervisory Authority activities in 2020

Under the GDPR, national Supervisory Authorities (SAs) have a duty to cooperate to ensure the consistent application of data protection law. In cases that have a cross-border component, the SAs of the European Economic Area (EEA), i.e. the 27 EU Member States plus Iceland, Norway and Liechtenstein, have a range of tools at their disposal to facilitate harmonisation.

These tools are:

- Mutual assistance;
- Joint operations;
- The One-Stop-Shop cooperation mechanism.

### 6.1. CROSS-BORDER COOPERATION

The GDPR requires the EEA SAs to cooperate closely to ensure the consistent application of the GDPR and protection of individuals' data protection rights across the EEA.

One of their tasks is to coordinate decision-making in cross-border data processing cases.

#### 6.1.1. Preliminary procedure to identify the Lead and Concerned Supervisory Authorities

Before starting a One-Stop-Shop (OSS) procedure for a cross-border case, it is necessary to identify the Lead Supervisory Authority (LSA) and the other Concerned Supervisory

Authorities (CSAs). The LSA leads the investigation and drafts the decision, while the CSAs have the opportunity to raise objections.

The LSA is identified as the SA of the EEA country where the data controller or processor under investigation has its main establishment. To identify a controller's or processor's main establishment, one key criteria is the place of central administration. Further information on this subject is available in the [Article 29 Working Party Guidelines for identifying a controller's or processor's LSA](#), endorsed by the EDPB at its first plenary meeting on 25 May 2018.

The EDPB created workflows in the Internal Market Information System (IMI) to enable SAs to identify their respective roles. This IT platform is used to support cooperation and consistency procedures under the GDPR. The main purpose of this procedure is to define roles at an early stage.

In case of conflicting views regarding which SA should act as LSA, the EDPB acts as a dispute resolution body and issues a binding decision. From 1 January 2020 to 31 December 2020, there were 742 instances in which LSAs and CSAs were identified. In 2020, all decisions were made in consensus and no dispute under Article 65.1.b GDPR was brought to the EDPB.

## 6.1.2. Database regarding cases with a cross-border component

A case with a cross-border component is registered in a central database via the IMI and may occur in several situations:

- When the data controller or processor has an establishment in more than one Member State;
- When the data processing activity substantially affects individuals in more than one Member State; and/or
- When SAs are simply exchanging information, i.e. providing each other with mutual assistance.

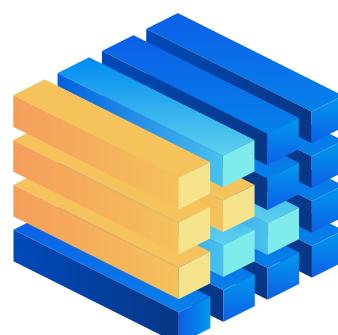
Between 1 January and 31 December 2020, there were 628 cross-border cases out of which 461 originated from a complaint, while 167 had other origins, such as investigations, legal obligations and or media reports.

## 6.1.3. One-Stop-Shop mechanism

The OSS mechanism demands cooperation between the LSA and the CSAs. The LSA leads the investigation and plays a key role in the process of reaching consensus between the CSAs, in addition to working towards reaching a coordinated decision about the data controller or processor.

The LSA must first investigate the case while taking into account national procedural rules, ensuring that the affected individuals are able to exercise their rights. During this phase, the LSA can gather information from another SA via mutual assistance or by conducting a joint investigation. The IMI also gives the LSA the opportunity to informally communicate with all CSAs to collect relevant information.

Once the LSA has completed its investigation, it prepares a draft decision, which it then communicates to the CSAs. They have the right to object. This either leads to a revised draft decision or, if no consensus can be found, the EDPB acts as a dispute resolution body and issues a binding decision. The LSA must adopt its final decision on the basis of the EDPB's decision. If the CSAs do not object to either the initial draft or the revised decision, they are deemed to agree with the draft decision.



Between 1 January 2020 and 31 December 2020, there were 203 draft decisions, from which resulted 93 final decisions.

The IMI offers different procedures that can be followed when handling OSS cases:

- Informal consultation procedures;
- Draft decisions or revised decisions submitted by the LSA to the CSAs; and/or
- Final OSS decisions submitted to the CSAs and the EDPB.

The EDPB has published a new public [register](#) of the decisions taken by LSAs pursuant to the OSS as a valuable resource to showcase how SAs work together to enforce the GDPR in practice. The relevant LSAs have validated the information in this register in accordance with the conditions provided by their national legislation.

#### **6.1.4. One-Stop-Shop decisions**

According to Art. 60(7) GDPR, the Lead Supervisory Authority (LSA) shall inform the EDPB of the final decision taken concerning cross-border cases in the context of the OSS mechanism. According to the GDPR, there is no obligation to make these final decisions public.

Nonetheless, during the 28th Plenary meeting of the EDPB on 19 May 2020, the Members of the EDPB decided to publish a [register](#) on the EDPB website relating to these decisions and containing the maximum amount of information possible taking into consideration national limitations.

The register offers an exceptional opportunity to read final decisions taken by, and involving, different SAs in a cross-border context. These decisions often contain interesting guidance on how to comply with the GDPR in practice. The register contains both final decisions and its summaries prepared by the EDPB Secretariat and duly approved by LSAs.

This section contains a selection of examples of Art. 60 GDPR final decisions taken from the EDPB's public register. The first section contains some cases where SAs handed out administrative fines in accordance with Art. 83 GDPR when data controllers did not comply with the GDPR. The second section provides summaries of some other final decisions in cases where SAs did not issue administrative fines, but provided guidance on the interpretation of specific provisions of the GDPR.

As the register was made public in 2020, this Annual Report makes reference to final decisions from the entry into application of the GDPR in 2018 until the end of 2020, during which 168 final decisions were adopted.

##### **6.1.4.1. Selection of cases involving administrative fines**

Consistent enforcement of data protection rules is central to a harmonised data protection regime. Once an infringement of the GDPR has been established based on the assessment of the facts of the case, the competent SA must identify the most appropriate corrective measure to address the infringement. Administrative fines are one of the most powerful enforcement measures the SAs can adopt, together with the other measures in Art. 58 GDPR.

##### **Lawfulness of processing / Personal data breach/Security of processing/ Administrative fines**

###### **LSA: Lithuanian SA**

Year of decision: 2019

This case concerned the taking of screenshots by the data controller when a user made an online payment using its service. The user, however, was not notified about the

screenshots being taken. The screenshots recorded personal data of the payer, such as their name and surname, numbers, recent transactions, loans, amounts, mortgages and so on. Moreover, the data controller had provided access to personal data to individuals who were not authorised and did not report the relevant data breach.

Regarding the processing of personal data in screenshots, the LSA considered that this processing by the controller went beyond what was necessary for the performance of the payment service and was also stored for a longer period than necessary. The controller failed to demonstrate the need to collect such an amount of personal data. Moreover, users were not informed of the processing. Therefore, the LSA considered that the processing of personal data was unlawful and that it violated the data minimisation and storage limitation principles.

Regarding the unauthorised access to the personal data, due to a security breach, unauthorised individuals had access to the data concerned, since access could be gained on the controller's website merely by using the identity of the transaction number. The LSA found that the controller failed to implement the appropriate technical or organisational measures to ensure data security. The LSA found that the data controller failed to notify the SA of the relevant data breach as required by Art. 33 GDPR without providing sufficient explanation of that failure to notify.

The LSA decided to impose a fine of EUR 61,500 (2.5% of the controller's total annual worldwide turnover).

## Lawfulness of processing

### LSA: Maltese SA

Year of decision: 2019

The complainant lodged a complaint with the CSA alleging that the controller kept sending marketing communications to the

complainant even though he had previously objected to the processing of his data for marketing purposes. The controller as internal procedure accepted requests from data subjects only when the requests were made using the same email address the users had used to open their accounts.

Through its investigations, the LSA found out that the controller could not find the first email sent by the complainant to object to the processing of his data for marketing purposes even if this email was sent from the email address used by the user to open his account. The data controller admitted that there was a possibility that the email had not been received or had not been dealt with properly.

Following the receipt of further unsolicited marketing communication, the complainant objected several more times. These emails were sent from email addresses different from the one used to open his account. Even if the controller was thus not able to comply with the data subject's request as it could not identify him, the controller decided to block the complainant's account from receiving marketing communications. From the investigation, it appeared that the controller did not have any internal procedures for handling data subject requests. In addition, the controller did not cooperate with the LSA, which had to wait months to receive the requested submissions.

The LSA found that the controller infringed Art. 21 GDPR by not having adequate procedures put in place to deal with the complainant's request to exercise his right to object. The LSA decided that the controller also infringed Art. 31 GDPR by not cooperating with the LSA. Consequently, the LSA imposed an administrative fine of EUR 15,000 on the controller. A EUR 2,000 administrative fine was also imposed on the controller for having breached several provisions of national law relating to unsolicited communications.

## **Transparency and information / Administrative fines**

### **LSA: Latvian SA**

Year of decision: 2019

The complainant alleged that he did not receive information on the identity of the controller before submitting his order on an online retail platform. Moreover, the complainant contended that the privacy policy available on the website was not in conformity with the GDPR.

During its investigation, the LSA found that the controller was a Latvian company performing retail sales through several websites, including the one used by the complainant to order his goods. After establishing the identity of the controller, the LSA found that the privacy policy on the website did not provide information on the identity of the controller, the legal basis of the data processing, its purposes and the way data subjects' consent was collected.

The LSA found that the controller did not comply with its obligations under the GDPR and imposed a fine of EUR 150,000.

## **Principles relating to processing of personal data / Transparency and information / Administrative fines**

### **LSA: French SA**

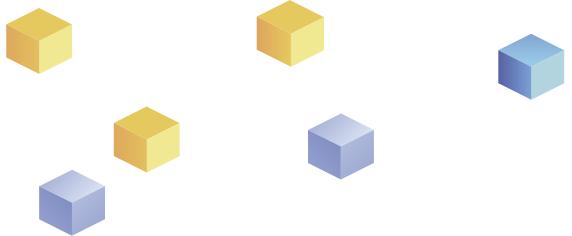
Year of decision: 2019

The controller conducted a full and permanent recording of all phone calls from its customer service employees without their ability to object. The controller did not prove that it had limited this processing to what was necessary for the purposes of assessing and training its employees. The controller also recorded the bank details of customers placing orders by telephone when recording its employees' conversations for

training purposes and stored such data in clear text in its database for 15 days.

The controller collected copies of Italian health cards and valid identity cards for anti-fraud purposes. The controller also stored a significant amount of personal data of customers who had not connected to their account in over 10 years and of individuals who had never placed an order on the company's website. After the expiry of the storage period for customers' data, the company kept some of their data such as their email address and password in a pseudonymised form for the alleged purpose of enabling customers to reconnect to their accounts. The controller did not inform its customers that their data was transferred to Madagascar. The controller only cited in its privacy policy one legal basis for processing - consent - whereas it conducted several processing operations on different legal bases. The controller did not inform its employees individually of the recording of their telephone calls. The controller accepted user account passwords with eight characters and only one category of characters. It also requested its customers to provide it with a scan of the bank cards used for ordering for anti-fraud purposes. These were subsequently stored by the company in clear-text and containing all of the credit card numbers for six months.

The LSA considered that the controller's recording of all phone calls from its customer service employees, including the bank details of customers placing orders by telephone, and the collection of Italian health cards, which contain more information than the identity card, were not relevant to combat fraud and was excessive. It concluded that it was a breach of the data minimisation principle of Art. 5(1)(c) GDPR. The LSA concluded that the company's storage of a significant amount of personal data of former customers and prospects over long periods that exceeded the purposes for which data were processed violated the storage limitation principle of Art. 5(1)(e) GDPR. The LSA considered that the controller had not informed customers up to a specific date of the transfers of



data to Madagascar nor of the respective legal basis for each processing operation. The LSA also decided that the controller did not adequately inform its employees of the recording of their telephone calls.

All these failings constituted a breach of Art. 13 GDPR (information provided to data subjects). The LSA considered that the type of password authorised by the company did not take sufficient security measures to ensure the security of its customers' bank data, which violated Art. 32 GDPR (security of processing). The LSA provided a detailed indication on how passwords can meet the threshold for "strong passwords". The LSA decided to impose a compliance order on the controller to remedy its breaches of the principles of data minimisation, data storage limitation, requirement to inform data subjects and to ensure data security. It associated the compliance order with a periodic penalty payment of EUR 250 per day of delay on expiry of a period of three months following the notification of this decision.

The LSA also imposed on the controller an administrative fine of EUR 250,000. The LSA further decided to make its decision public on its website, identifying the company by name, for a period of two years.

## **Lawfulness of processing / Transparency and information / Right to erasure / Administrative fines**

### **LSA: Spanish SA**

Year of decision: 2020

The LSA received two separate complaints related to the processing of personal data through the controller's mobile app for Android, from complainants who received prank calls via the controller's application. This app allowed its users to carry out telephone pranks on third parties. The user selected a prank, and a third party (a "victim") was then contacted by

phone through a hidden number via the controller's application. The audio of the conversation was recorded and made available to the user. The user was able to share the recording on social media. The third party was not asked for consent for processing of his/her personal data.

The LSA considered that the controller carried out the processing without first informing data subjects, namely, the people receiving the prank call. As such, the data subjects were not aware of the controller's processing of their personal data. The controller claimed that it processed personal data based on the legitimate interest as per Art. 6(1)(f) GDPR. However, the controller did not inform data subjects of its use of the legitimate interests of the controller or of a third party as a legal basis for processing.

The LSA decided that the controller's processing of data was not necessary for the purposes of the protection of its legitimate interests, nor did these interests outweigh the fundamental rights and freedoms of the data subject to the protection of his/her personal data. The LSA concluded that the legitimate interest referred to in Art. 6(1)(f) GDPR could be used as a legal basis for the processing of personal data in this case. Consent also could not serve as a legal basis in this data processing act. The conditions it requires, such as being informed, were not met. The LSA concluded that the processing carried out by the controller could not, under any circumstances, be regarded as lawful and violated Art. 6 GDPR.

For the infringement of Arts. 13 and 14 GDPR and the infringement of Art. 6 GDPR, the LSA imposed two administrative fines, each of EUR 20,000.

The LSA also required the controller to ensure compliance with the rules on personal data protection relating to its processing operations within three months, including the information it provides to its clients and the procedure by which they must give their consent to the collection and processing of their personal data.



## Personal data breach / Administrative fines

### LSA: United Kingdom SA

Year of decision: 2020

On 22 June 2018, an unidentified attacker gained access to the data controller's IT systems via CAG (a tool that allows users to remotely access a network) and maintained this ability to access without being detected until 5 September 2018. After gaining access to the wider network, the attacker traversed across the network. This culminated in the editing of a JavaScript file on the controller's website. The edits made by the attacker were designed to enable the exfiltration of cardholder data from that website to an external third-party domain, which the attacker controlled. The controller was alerted by a third party about the exfiltration of personal data from the controller's website and then notified the LSA about the attack on 6 September 2018.

The controller estimated that 429,612 data subjects were affected. The affected categories of personal data were username and passwords of contractors; employees and members of an executive club; customer names and addresses; and unencrypted payment card data including card numbers, CVV numbers and expiry dates. The controller took immediate measures to mitigate and minimise any damage suffered by the data subjects by implementing remedial measures, including notifying banks and payment schemes, the data subjects and data protection regulators; cooperating with regulatory and governmental bodies; and offering reimbursement to all customers who had suffered financial losses as a direct result of the theft of their card details. The controller also implemented a number of remedial technical measures to reduce the risk of a similar attack in the future.

The LSA found that the controller failed to process the personal

data of its customers in a manner that ensured appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures, as required by Art. 5(1)(f) and Art. 32 GDPR. The LSA concluded that there are a number of appropriate measures that the controller could have considered to mitigate the risk of an attacker being able to access the controller's network. The LSA considered that each step of the attack could have been prevented, or its impact mitigated, by the controller's implementing one or more of those appropriate measures that were open to the controller. The LSA also considered that, had the controller performed more rigorous testing or internal penetration tests, it would have likely detected and appropriately addressed many of the data security problems identified.

The LSA concluded that the infringements constituted a serious failure to comply with the GDPR. The LSA decided to impose an administrative fine of GBP 20,000,000 on the controller after having taken into account a range of mitigating factors and the impact of the COVID-19 pandemic.

## Personal data breach / Administrative fines

### LSA: United Kingdom SA

Year of decision: 2020

The personal data breach in this instance related to exposed personal details, such as names, payment card numbers, expiration dates and CVV numbers. 9,400,000 EEA data subjects, of whom 1,500,000 were in the UK, were notified as having been potentially affected by the personal data breach. The personal data breach related to compromised bankcard details and transaction fraud on bank accounts. One bank suggested that around 60,000 individuals' card details had been compromised, while another bank suggested that around

6,000 payment cards had needed to be replaced as result of the controller's transaction fraud. The controller received around 997 complaints from individuals claiming economic loss and/or emotional distress. The controller was not able to provide a detailed analysis of the individuals affected to the SA.

The LSA found that the controller had failed to process personal data in a manner that ensured appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures as required by Art. 5(1)(f) and Art. 32 GDPR. In addition, the LSA found that the controller failed to detect and remediate the breach in a timely manner or provide a fully detailed analysis of the individuals affected to the LSA within 72 hours of having detected the personal data breach. Furthermore, the LSA considered mitigation factors, such as the fact that the controller forced password resets across all its domains and created a website where customers could access information about the personal data breach.

In view of the above, the LSA imposed an administrative fine of GBP 1,250,000 on the controller.

## Personal data breach / Security of processing / Administrative fines

### LSA: United Kingdom SA

Year of decision: 2020

The controller for the data processing activity at stake acquired a company whose IT systems were infiltrated by an attacker before the acquisition. The controller was not aware of the infiltration during the acquisition, nor did it become aware of this afterwards. The controller realised the infiltration once the attacker triggered an alert in relation to, amongst others, a table containing cardholder data. The attacker appeared to have obtained personal data in both an encrypted and unencrypted

form. The unencrypted personal data contained data from the guest profile, including reservation and consumption data of customers, while the encrypted information contained 18,500,000 encrypted passport numbers and 9,100,000 encrypted payment cards. Subsequently, the controller informed the data subjects and took steps to mitigate the effects of the attack. Finally, the controller notified the LSA of the personal data breach.

The LSA investigated the case and found that the controller did not ensure appropriate technical and organisational measures to ensure an appropriate level of security as required by Art. 5(1)(f) and Art. 32 GDPR. In particular, the LSA found that the controller did not sufficiently monitor the privileged accounts and the databases. In addition, the LSA found that the controller failed to ensure that the actions taken on its systems were monitored appropriately and that the controller did not apply encryption to all the passport numbers, as it should have.

The LSA, considering the relevant mitigating factors, imposed an administrative fine of GBP 18,400,000 on the controller.





### 6.1.4.2. Other cases on the interpretation of GDPR provisions

#### Lawfulness of the processing

##### LSA: North Rhine-Westphalia SA

Year of decision: 2018

The complainant stated they received postal advertising and tried to exercise their right of access and right to erasure. The complainant contacted their local SA as they deemed that the controller was wrongfully processing their personal data. The data used by the controller was collected from a publicly accessible register.

The LSA underlined that recital 47 and Art. 6(1)(f) GDPR provide for the possibility for data controllers to rely on legitimate interest for the processing of personal data for marketing purposes. As the data were already publicly accessible, the LSA argued that the data subject did not present any prevailing fundamental rights and freedoms, and neither were prevailing rights and freedoms apparent. The LSA decided that the processing of publicly available personal data for direct marketing purposes may constitute lawful processing according to Art. 6(1)(f) GDPR.

Regarding the data subject requests, the original access and erasure requests were filed before 25 May 2018 and Arts. 13 and 14 GDPR were thus not yet applicable. The LSA underlined that these articles require data controllers to inform data subjects of which source the personal data originate. The LSA requested that the controller provide this information for future advertising mail.

The LSA concluded that there was no GDPR infringement.

#### Request to erasure / Identity authentication

##### LSA: French SA

Year of decision: 2019

The complainant stated that the right to erasure had been refused by the controller. The controller requested a scan of the complainant's identity document and their signature, although neither of the two were required upon creating the relevant account.

The LSA found that the controller systematically requested that individuals provide a copy of an identity document for exercising their rights, regardless of their country of residence and without providing a basis for reasonable doubts as to the identity of the complainant according to Art. 12(6) GDPR. As such, the LSA found that the controller required disproportionate information for the purpose of verifying the identity of the data subject. The SA stated that it is disproportionate to require a copy of an identity document where the claimant has made their request where they are already authenticated. An identity document may be requested if there is a suspicion of identity theft or account piracy, for instance.

In addition, the LSA underlined that a controller may only store information needed for the exercise of individuals' rights until the end of the applicable legal limitation periods. During this period, the data have to be subject to an "intermediary" archiving on a support base separate from the active base with restricted access to authorised persons.

The LSA issued a reprimand against the controller.

## Interpretation of Art. 24 GDPR

### LSA: Czech SA

Year of decision: 2019

A complaint was filed with a CSA concerning the processing of personal data of the users of antivirus software provided by the controller, and specifically the protection granted to users of the free version of the software compared to that granted to the paying users.

In its inspection report, the LSA concluded that the inspected party failed to comply with Art. 5(2) and Art. 24(1) GDPR. This was interpreted as the obligation to take into account all relevant circumstances surrounding the processing and to adopt a set of measures to ensure that all personal data processing is carried out exclusively under pre-defined conditions that the controller is able to regularly check and enforce. This stemmed from the conclusion – based on Court of Justice of the EU jurisprudence - that the inspected party, despite its assertions to the contrary, was indeed processing personal data (such as IP addresses) and was acting as a data controller.

The controller filed several objections to the inspection report, arguing, amongst others, that no processing of personal data was involved, that it was not a data controller, and that sufficient information to properly show compliance with Art. 5(2) and Art. 24(1) GDPR was provided. The last objection was partially accommodated by the LSA, which concluded that only an infringement of Art. 24(1) GDPR had been ascertained, whereas no specific breach of Art. 5(2) GDPR followed from the documentation.

The controller was found to have violated Art. 24(1) GDPR.

## Request for access / Identity authentication

### LSA: Brandenburg SA

Year of decision: 2019

The complainant requested access to his personal data processed by the controller. The controller verified the data subject's identity, and subsequently informed the complainant that his account had been suspended due to a discrepancy between the information concerning the age on his account and the information he had provided for the verification of his identity for the request. Since he was 15 years old at the time and thus a minor, he was also asked to send parental consent, a copy of his identity card and a birth certificate to access his personal data. The complainant filed a complaint to the CSA on the understanding that the information he had provided for the verification process was wrongly used to suspend his account instead of being used for the process of giving access to personal information.

The controller underlined that at the time of the request there was no standardised process in place within the company for requests by minors, since the contractual relationship between the controller and the data subjects depends on the fact that the data subjects are adults. Shortly after the controller requested additional documentation for parental consent, this request was set aside and access to personal data was given to the complainant. Finally, further measures were taken by the controller to improve the data access process.



The LSA decided that the request for information was answered in due time and the controller's verification process had been modified in a suitable manner. The LSA therefore found that there was no infringement of the GDPR.

## **Lawfulness of publication - legitimate interest**

### **LSA: Czech SA**

Year of decision: 2019

The data subject filed a complaint with one of the CSAs alleging that the controller published his personal data on its social media page without a legal basis. The controller published information concerning the complainants and other data subjects, referring to debts that the controller was in charge of collecting, on its social media page. The abbreviated first name and the entire surname of the data subjects, as well as the status of debtor and the amount owed by them were specified.

The controller argued it did this on the basis of its legitimate interest. The LSA provided a detailed assessment of the conditions for legitimate interest to be a lawful legal basis. According to the LSA, the controller's legitimate interests must first of all be lawful, i.e., in compliance with legal regulations, and clearly formulated (not speculative). These legitimate interests also include economic interests, i.e., interest in securing the economic side of its business operations. The processing must also be necessary for the purposes of the legitimate interests of the respective controller or third party, i.e., it is not possible to achieve the same result by processing a narrower scope of personal data or infringing the data subjects' rights to a lesser degree. Finally, the interests or rights and freedoms of the data subjects should not take precedence over the alleged legitimate interests. The LSA explained that in this assessment it is also necessary to take into account the nature and importance of the controller's legitimate interests, the impact of the respective processing on the data subjects,

including the data subjects' reasonable expectations and any other protective measures applied by the controller.

The LSA decided that the controller had other less intrusive means to fulfil its interests. In addition, the interests and rights of the data subject prevailed over those interests, given the significant risk of adverse impact arising from the publication of negative information about the data subjects' financial situation. Such information could lead to the social exclusion of such persons and their family members, loss of employment and other negative implications. Moreover, data subjects had reasonable expectations of data not being disclosed.

As a result, the LSA considered that the interests of the controller or any third parties were outweighed by the data subject's interests and basic rights and freedoms requiring protection of personal data. The LSA ordered the controller to cease processing of the complainant's personal data and to remove the published personal data within 10 business days of the decision. The LSA also ordered the controller to submit a report to the LSA on the implementation of the order within five business days of its completion.

## **Data subject rights**

### **LSA: Hessen SA**

Year of decision: 2019

The complainant filed a complaint with the CSA contending that the controller did not comply with his access request within the one-month period, as established in Art. 12(3) GDPR.

When contacted by the LSA, the controller explained that the number and complexity of the data-related customer queries at the time of the request justified an extension of the one-month period. Additionally, by mistake, no notice of the extension had been sent to the complainant within the deadline. However, shortly after the deadline, the controller did

send the complainant a notice of the extension. The access request was complied with within the extended timeframe.

The LSA found that there was an infringement of Art. 15 GDPR since the controller did not comply with the complainant's access request in the established timeframe and issued a reprimand to the controller. However, the LSA considered that the controller had cooperated with the LSA during the investigation and notified the complainant of the justified need for an extended timeframe shortly after the due date and answered the request within the extended timeframe. Therefore, the LSA decided not to take any further measures against the controller.

## **Interpretation of Art. 12(6) GDPR concerning identity authentication**

### **LSA: Danish SA**

Year of decision: 2019

The complainant requested to have his personal data deleted from the controller's database. The controller replied that, before processing his erasure request, a proof of identification was necessary to confirm his identity. As the complainant refused to comply with the controller's demand, his data was not deleted.

The LSA found that the controller's procedure under which identification validation was required without exception when processing a data subject's request was not in conformity with Art. 12(6) and Art. 5(1)(c) GDPR. The LSA also found that, under the controller's procedure, data subjects had to provide more information than initially collected in order to have their request processed. Consequently, the controller's procedure for identification validation went beyond what was required and made it burdensome for data subjects to exercise their rights.

The LSA decided that the processing was not done in accordance with Art. 12(6) and Art. 5(1)(c) GDPR. It ordered the controller to decide within two weeks whether the conditions for erasure present in Art. 17 GDPR were met and, if so, to delete the complainant's data.

## **Adequately informing data subjects and securing their data**

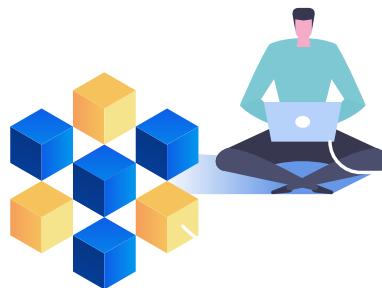
### **LSA: French SA**

Year of decision: 2019

The LSA conducted two on-site investigations at the controller's premises to audit the controller's compliance with the GDPR and tested the procedure set up by the controller to create an account.

The controller is a company offering subscriptions to educational magazines for children. On the basis of the investigation, the LSA found several GDPR infringements. First, several breaches of the obligation to inform data subjects, enshrined in Art. 12 and Art. 13 GDPR, were identified. No information relating to data protection nor a link to the controller's Terms and Conditions was given to data subjects upon registration or when placing an order. As a consequence, the information was considered to be not accessible enough. The Terms and Conditions did not include any information on the legal basis for processing, the retention period and the individual rights to restriction of processing, data portability, or to submit a claim to an SA. Although the target audience was French-speaking and the website is fully in French, the "unsubscribe" button in the newsletter and marketing emails was hyperlinked to a text in English, asking for confirmation. An additional hypertext link was included in the final page (titled "Clicking here"). The LSA considered this link misleading for the users, as clicking on it actually resulted in a new subscription.

Second, a breach of the obligation to comply with the request



to erase data was identified, as personal data was not erased systematically when requested by data subjects although there was no legal requirement to keep it and although users had been informed of the erasure of the data. Third, there was a breach of the obligation to ensure the security of data, concerning passwords, locking of workstations and access to data. More specifically, the password requirements and methods for processing the passwords were found to be non-compliant with the obligation to implement technical and organisational measures to ensure a level of security appropriate to the risk, since authentication was based on insufficiently complex passwords and obsolete hash algorithms. Additionally, the computer used by one of the database's administrators was configured to never automatically lock or go on sleep mode. With regard to access to data, the absence of specific identification (i.e., the use of the same account by several people) made it impossible to ensure access traceability.

The LSA ordered the controller to comply, within two months of the notification of the decision, with several specific instructions. First, the controller was ordered to provide full information to data subjects about the processing activities in an easily accessible manner. Additionally, the LSA ordered the controller to set up a procedure for unsubscribing that is compliant with Art. 12 and Art. 21 GDPR. Second, the controller was ordered to ensure the effectiveness of all requests to exercise the right of erasure. Third, the authority ordered the controller to take appropriate security measures to protect personal data and prevent access thereto by unauthorised third parties by setting up a new password policy, avoiding the transmission of passwords in clear text, ensuring that workstations go on sleep mode and setting up individual accounts.

## Lawfulness of data processing

### LSA: French SA

Year of decision: 2020

The complainants encountered difficulties exercising their right to object to direct marketing and rights of access and portability.

The LSA found out during the investigation that an incident arose during the migration of the controller's consent management tool for marketing communications, causing consents not given/withdrawn considered as given/not withdrawn, and the users' communication preferences not to be taken into account in the controller's communication campaigns.

Although the LSA noted that the problem had been solved and that the users' communication preferences had been restored, it stemmed from this incident that, before the migration of its consent management tool, the controller had not implemented the necessary measures as required by Art. 24 GDPR.

The LSA also found that the controller's procedure to process access requests was not fully compliant with Art. 32 GDPR. Indeed, the LSA noted that, in the absence of a client account, the username and password for connection to content containing personal data were sent to data subjects via the same channel. The LSA stated that it was the controller's duty to communicate the username and password for connection via two different communication channels.

As such, the controller was asked to modify this procedure. The LSA determined that the controller had improved the procedures to handle data subject rights requests and trained employees on such procedures.

The LSA issued a reprimand to the controller.

## Data subject rights in the context of marketing

### LSA: Hungarian SA

Year of decision: 2020

The complainant lodged a complaint against the controller with one of the CSAs after receiving unsolicited marketing messages. The complainant asked to unsubscribe on several occasions without success.

The LSA requested that the complainant make a statement within eight days to disclose his identity to the controller in the course of the procedure, warning that without disclosing his identity, the investigation could not be conducted. The LSA also requested a copy of the erasure request addressed to the controller, as well as copies of any other communication and correspondence with the controller and the controller's response to the erasure request.

The LSA repeated this request a number of months later as there was no response from the complainant. In the absence of a response, the LSA examined the documents made available to it by the CSA. It was not possible to establish from the screenshots enclosed when the complainant unsubscribed from the controller's newsletter or on how many occasions. The documents were not dated, and email addresses were not visible or available. The screenshots of the electronic newsletters of the controller did not reveal the addressee nor the email address that they were sent to.

As the complainant's request remained unverified, no decision establishing an infringement was made. The LSA rejected the complaint without an investigation of merit.

## Right to object / Right to erasure

### LSA: Austrian SA

Year of decision: 2020

The complainant informed the CSA that he had been receiving advertising emails for months. Attempts to unsubscribe had been unsuccessful and appeared to generate further spam emails. The complainant subsequently contacted the CSA to request assistance with enforcing his objection to the unsolicited spam emails.

The complainant did not contact the controller regarding the assertion of his rights as a data subject concerned. The LSA considered that, following Art. 12 GDPR, the rights under Art. 15 to Art. 22 GDPR require a request by the data subject. Such requests for information or objection were not made to the controller. Therefore, the complaint was dismissed and the CSA to which the complaint was submitted was called to take the final decision in accordance with Art. 60(8) GDPR and to notify the complainant and the controller.

## Right of access

### LSA: Cypriot SA

Year of decision: 2020

The complainant sent an email to the controller requesting the closure of his account and access to his data on the basis of Art. 15 GDPR. According to the complainant, the controller did not reply to the access request, so he lodged a complaint with the SA.

The LSA found that the email sent by the complainant, wherein he requested access to his data, was never received as it was flagged by the email security service and categorised as spam due to the applied information security IT measures for emails

received from outside the controller. The account manager who also received the email assumed that it had an informative character and was under processing, since the established procedure for an account closure is to be forwarded only to the team responsible for this (Customer Support Team).

Since the controller affirmed that it was working with the IT department to find a solution to avoid similar incidents in the future and that it planned on organising training sessions for staff that interact with the clients, the LSA decided not to take further actions regarding this matter.

### **6.1.5. Mutual assistance**

The mutual assistance procedure allows SAs to ask for information from other SAs or to request other measures for effective cooperation, such as prior authorisations or investigations.

Mutual assistance can be used for cross-border cases subject to the OSS procedure, either as part of the preliminary phase, to gather the necessary information before drafting a decision or for national cases with a cross-border component.

The IMI enables the use of either informal mutual assistance without any legal deadline or the use of formal mutual assistance. In the latter case, according to the GDPR, the SA from which information has been requested has a legal deadline of one month to reply.

Between 1 January 2020 and 31 December 2020, SAs initiated 246 formal mutual assistance procedures. They initiated 2,258 informal such procedures.

### **6.1.6. Joint operations**

The GDPR allows SAs to carry out joint investigations and joint enforcement measures. Similar to the Mutual Assistance

procedure, SAs can use joint operations in the context of cross-border cases subject to the OSS procedure, or for national cases with a cross-border component.

In 2020, SAs carried out one joint operation.<sup>1</sup>

## **6.2. NATIONAL CASES**

SAs have different investigative, advisory and corrective measures at their disposal to ensure entities within their countries apply data protection law correctly and consistently. Such measures include the following:

- Issuing warnings to a controller or processor where its intended processing operations are likely to infringe the GDPR;
- Issuing reprimands to a controller or processor where processing operations have infringed the GDPR;
- Ordering the controller or processor to comply with a data subject's request or to bring processing operations into compliance with the GDPR;
- Imposing processing limitations, bans or fines.

### **6.2.1. Some relevant national cases with exercise of corrective powers**

SAs play a key role in safeguarding individuals' data protection rights. They can do this through exercising corrective powers. The EDPB website includes a selection of [SA supervisory actions](#). This section of the Annual Report contains a non-exhaustive list of certain enforcement actions in different EEA countries. Several cases highlighted a lack of proper technical and organisational measures for processing personal data securely, which led to data breaches. Many other cases revolved around data processing without a data subject's consent. Some significant incidents involved the unlawful processing of special categories of personal data, such as health data. Numerous cases also involved data subjects who could not

effectively exercise their rights, such as the right of access, the right to erasure and the right to object to a processing act. The entities fined were from both the private and the public sectors.

### **6.2.1.1. Austria**

The Austrian SA carried out multiple investigations and gave several warnings during 2020. For example, the SA carried out investigations into various data controllers that operate customer loyalty programmes. The controllers were seeking the consent of data subjects to process their personal data for the purpose of profiling and to personalise advertising. The request for consent was placed at the end of the registration form of the customer loyalty programme. Among other things, it was ruled that the requested consent was invalid as an average data subject would assume that a signature field placed at the end of a customer loyalty programme registration form is a signature to confirm the registration for the programme and not a signature to provide the consent for the processing of personal data. The controllers appealed this formal decision, meaning the case is still pending before the respective Austrian courts.

The Austrian SA also carried out investigations into the Public Employment Service of Austria (AMS). The AMS used an algorithm to evaluate the employment opportunities of unemployed people. It was ruled that there was no sufficient legal basis for using such programmes and that the personal data processing of unemployed people for this purpose was unlawful. The AMS appealed this formal decision and the Austrian Federal Administrative Court subsequently ruled that, contrary to the opinion of the Austrian SA, a sufficient legal basis exists for this processing. The case is currently pending before the Austrian Administrative High Court.

On 11 November, the Austrian SA issued a warning to the Federal Ministry of Social Affairs, Health, Care and Consumer Protection noting that the intended processing operations in

the context of the electronic COVID-19 vaccination passport were likely to violate the GDPR. The scope of the encroachments on the fundamental right to data protection were not clear from the legislation itself, however, provisions relating to the vaccination passport did not meet certain GDPR requirements, particularly with regard to transparency, the allocation of roles, data subject rights and statistical evaluations.

### **6.2.1.2. Belgium**

The Belgian SA published 31 decisions in 2020. This section lists some key decisions.

On 29 May, the Belgian SA imposed a fine of EUR 1,000 on a controller for not responding to a request from a citizen to object to the processing of his data for marketing purposes and for not collaborating with the SA.

On 8 June, the Litigation Chamber of the Belgian SA issued a fine of EUR 5,000 to a candidate in local elections for using the staff registry of a Municipality to send election propaganda, in the form of a letter, to staff members. The Belgian Municipality in question filed the complaint against the candidate.

On 16 June, the Belgian SA imposed a fine of EUR 1,000 on an association that, on the basis of its legitimate interest according to Art. 6(1)(f) GDPR, sent direct marketing messages to former and current donors for its fundraising efforts. The administrative fine was imposed following a complaint lodged with the Belgian SA by a former donor of the association as the association had not complied with the request for data erasure addressed by the individual to the data controller pursuant to the right to erasure and the right to object to processing. The Litigation Chamber thus decided that the data controller had infringed multiple GDPR provisions.

On 19 June, the Belgian SA issued a fine of EUR 10,000 to a controller for sending a direct marketing message to the wrong person and for not responding adequately to the data subject's



subsequent request for access to his data.

On 14 July, the Belgian SA imposed a EUR 600,000 fine on Google Belgium for not respecting the right to erasure of a Belgian citizen, and for a lack of transparency in its request form to delist.

On 30 July, telecom operator Proximus was fined EUR 20,000 for several data protection infringements regarding personal data processing for the purpose of publishing public telephone directories.

On 8 September, the SA issued a warning and reprimand to a regional public environmental institution for wrongful processing of personal data from the National Register. The Litigation Chamber of the Belgian SA may not impose an administrative fine on a Belgian public institution or any other government body as this was excluded by the Belgian legislator.

On 24 November, the Belgian SA issued a fine of EUR 1,500 for unlawful processing of personal data through a video surveillance system. The Belgian SA also concluded that the positioning of the cameras in the video system constituted an infringement of the data protection by design principle.

### 6.2.1.3. Bulgaria

The Bulgarian SA experienced an increase in the number of complaints received and the actions taken in 2020. The Bulgarian SA issued a total of 426 decisions as a result of complaints it handled, and imposed administrative sanctions amounting to a total of BGN 518,700 (EUR 265,207). Most violations were made by data controllers processing personal data via established video surveillance systems as well as in the sphere of telecommunication services, media, banks and marketing companies. This section expands upon a selection of interesting cases.

- Several cases concerned political parties or other organisations, which were involved in the procedure set for organising the EU parliamentary and local elections, where they submitted lists with supporters to participate in the elections and did not set clear procedures for verifying the personal identification data entered in the list, thus allowing falsification of signatures and the misuse of the Unified Civil Number of Bulgarian citizens. Since the cases concerned one or two individuals, the lack of procedure did not affect a large number of citizens, however in some of cases the parties in question had already been sanctioned for similar violations;
- A communal services provider was sanctioned for misusing an individual's personal data in case of debt insolvency, which led to the involvement of a private bailiff and a consequent payroll seizure. When imposing the fine, the Bulgarian SA considered the serious adverse effect suffered from the individual as a result of the violation and negligence with which the individual's personal data was handled by the employee and the practice on similar cases with the same type of violations;
- A magistrate, being a public person, issued a complaint about the publishing of a document, submitted by him by electronic media, without blurring his signature. In this case, the Bulgarian SA stated that despite the clear role of the electronic media as a provider of information for public interest purposes, leaving the signature of the public person had no added value and thus should have been blurred by the controller when publishing the provided document. The SA also considered that the violation was not the first one for this electronic media and the person concerned suffered negative consequences. The Bulgarian SA imposed an administrative sanction on the data controller and ordered it to bring its processing operations into compliance with the GDPR by minimising the published data;
- The Bulgarian SA handled a case about the requested erasure of a businessman's arrest photos, published by the media, who was acquitted by the court for corruption;

- Another case pertained to the dissemination of personal data by a state authority in connection with a corruption signal submitted to it;
- The Bulgarian SA also handled a case about a person who served a prison sentence and, once the 10-year statute of limitations expired, requested erasure of their personal data due to the expired public interest.

#### **6.2.1.4. Cyprus**

The Cypriot SA fined LGS Handling Ltd, Louis Travel Ltd and Louis Aviation Ltd (Louis Group of Companies) EUR 82,000 for the lack of legal basis of the “Bradford Factor” tool, which was an automated tool used to score the sick leave of employees. The Cypriot SA launched an investigation after the employees’ trade union lodged a complaint. Importantly, it had not been established that the legitimate interest of the controller overrode the interests, rights and freedoms of its employees.

On 17 June, the Cypriot SA imposed a fine of EUR 15,000 on the Bank of Cyprus Public Company Ltd for the loss of a client’s data, which specifically infringed Arts. 5(1)(f), 5(2), 15, 32 and 33 GDPR.

#### **6.2.1.5. Czech Republic**

The Czech SA fined a used car dealer CZK 6,000,000 for repeatedly sending unsolicited commercial communications. This was the highest fine the office imposed for this kind of breach. The company continually distributed electronic commercial communications to recipients who had not granted consent.

#### **6.2.1.6. Denmark**

Unlike in other EEA jurisdictions where the SAs have the authority to issue administrative fines themselves, in Denmark,

the Danish SA first investigates a data protection legal violation and then reports it to the police. The police then investigate whether there are grounds for raising a charge and finally a court decides on a possible fine.

In June, the Danish SA proposed that the Municipality of Lejre be fined DKK 50,000 for failing to comply with its obligation as a data controller to implement appropriate security measures. Its department called the Centre for Children and Young People had a fixed practice where meeting minutes containing personal information of a sensitive and protected nature, including information about citizens under the age of 18, had been uploaded on the Municipality’s employee portal where a large part of the employees could access this. In July, the Danish SA reported ARP-Hansen Hotel Group to the police and proposed a fine of DKK 1,100,000 for the failure to delete approximately 500,000 customer profiles, thus violating the storage limitation requirement in Art. 5(1)(e) GDPR.

In December, the Danish SA reported the Municipality of Guldborgsund to the police and proposed a fine of DKK 50,000. The Municipality had mistakenly sent a decision via Digital Post containing information about the complainant’s child’s place of residence to the complainant’s child’s father, even though the father had been deprived of custody, thus amounting to a security breach that had major consequences for the complainant and the child. The Municipality had failed to notify the complainant and the SA of the security breach.

#### **6.2.1.7. Estonia**

On 30 November, the Estonian SA granted a warning, with a one-day compliance deadline and a penalty of EUR 100,000, to three pharmacy chains that had allowed people to view the current prescriptions of other people in the e-pharmacy environment, without their consent, on the basis of access to their personal identification code.

### 6.2.1.8. Finland

This section sets out five pertinent instances in which the Finnish SA imposed fines for violations of data protection law.

On 18 May, the sanctions board imposed three administrative fines. First, for deficiencies in information provided in connection with change-of-address notifications, the board fined Posti Oy EUR 100,000. Second, because it had neglected to conduct a Data Protection Impact Assessment for the processing of employee location data, the sanctions board imposed an administrative fine of EUR 16,000 on Kymen Vesi Oy. Third, the board imposed a fine of EUR 12,500 on a company because it had collected job applicants' personal data unnecessarily.

On 26 May, the Finnish SA imposed an administrative fine on Taksi Helsinki Oy for violations of data protection legislation. The company had not assessed the risks and effects of personal data processing before adopting a camera surveillance system that recorded audio and video in its taxis. The Finnish SA noted deficiencies in the information provided to customers and the documentation of personal data processing. The sanctions board imposed an administrative fine of EUR 72,000 on Taksi Helsinki.

In July, the sanctions board of the Finnish SA imposed an administrative fine on Acc Consulting Varsinais-Suomi for sending direct electronic marketing messages without prior consent as well as neglecting the rights of data subjects. The company did not respond to or implement the requests concerning the rights of data subjects, and it was not able to prove that it had processed personal data legally. The sanctions board therefore imposed a financial sanction of EUR 7,000 in addition to several corrective measures for the company to complete.

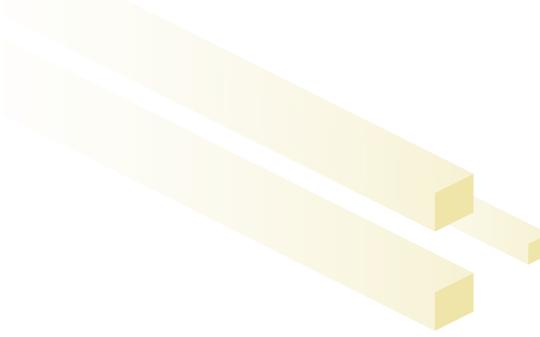
### 6.2.1.9. France

France had several important cases with comparably large fines in 2020. Such cases pertained to the following entities: SPAROO, Carrefour France and Carrefour Banque, Google LLC and Google Ireland Ltd, and Amazon Europe Core.

In applying the one-stop-shop mechanism, the French SA acted as the LSA in a cross-border enforcement case involving thirteen EEA countries. The French SA found that SPAROO, which specialises in the online shoe sales sector, had failed to comply with the following obligations: to adhere to the data minimisation principle; to limit the data retention period; to inform data subjects adequately about how their personal data would be processed; and to ensure data security. In August, the French SA imposed a fine of EUR 250,000 and issued an injunction to the company to comply with the GDPR.

In November, the French SA issued fines of EUR 2,250,000 to Carrefour France and EUR 800,000 to Carrefour Banque for violations of data protection law. Most of the violations pertained to customer information relating to a loyalty programme and the related credit card (Pass card). The companies failed in their obligation to inform data subjects about data processing according to Art. 13 GDPR related to joining the loyalty programme or the Pass card. The information given was not easily accessible, easily understandable or complete. The companies also failed to adhere to French data protection law relating to cookies. The relevant websites installed advertising cookies without first obtaining the user's consent.

Carrefour France failed to comply with the obligation to limit the data retention period of its customers' personal data. It also infringed its obligation to facilitate the exercise of data subject rights and failed to respond to certain requests for access to personal data and deletion requests. Carrefour Banque infringed its obligation to process personal data fairly under Art. 5 GDPR as it processed more personal data than what it had indicated to people subscribing to the Pass card.



On all points, the companies changed their practices during the procedure and committed significant resources to make the necessary modifications to bring them into compliance with the GDPR.

On 7 December, the French SA fined the companies Google LLC and Google Ireland Ltd a total of EUR 100,000,000 for having placed advertising cookies on the computers of users of the search engine google.fr, without obtaining prior consent and without providing them with adequate information.

The French SA justified the fines with regard to the seriousness of the breach of the French Data Protection Act. It also highlighted the scope of the search engine Google Search in France and the fact that the practices of the companies affected almost 50 million users. It noted the companies generated significant profits deriving from the advertising income indirectly generated from data collected by the advertising cookies. The French SA noted that the companies had stopped automatically placing advertising cookies when a user arrived on the page google.fr after an update in September 2020. The French SA, however, noticed that the new information banner set up by the companies when a user arrived on the page google.fr still did not allow the users living in France to understand the purposes for which the cookies were used and did not let them know that they could refuse these cookies. As a consequence, in addition to the financial penalties, the French SA also ordered the companies to adequately inform individuals, in accordance with the French Data Protection Act, within three months of the notification of the decision. Failing that, the companies must pay a penalty payment of EUR 100,000 for each day of delay.

Similar to the Google enforcement action, on 7 December, the French SA fined Amazon Europe Core EUR 35,000,000 for having placed advertising cookies on users' computers from the page amazon.fr, both without obtaining their prior consent and without providing them with adequate information about

the personal data processing. The amount of the fine, and the decision to make it public, were justified by the seriousness of the breaches observed.

The French SA noted recent developments made on the site amazon.fr and, in particular, the fact that now no cookie is placed before obtaining the user's consent. The new information banner set up, however, still did not allow the users living in France to understand that the cookies are mainly used to personalise advertisements. Moreover, users were still not informed that they could refuse these cookies. In addition to the financial penalty, the French SA also ordered the company to adequately inform individuals per the French Data Protection Act, within three months of the notification of the decision. Otherwise, the company must pay a penalty payment of EUR 100,000 for each day of delay.

### 6.2.1.10. Germany

Germany has both a national (federal) SA and regional SAs. Three noteworthy cases involved enforcement actions by regional German SAs. The Lower Saxony SA imposed a fine of EUR 65,500 on a pharmaceutical manufacturer for using unsuitable and outdated software components on its website, equating to inadequate technical measures for the protection of personal data and thus breaching Art. 32(1) GDPR. The Berlin SA imposed a fine of EUR 6,000 on the regional association of a right-wing political party (the data controller) for the unlawful publication of personal data. The Hamburg SA imposed a fine of EUR 35,258,708 on H&M for data protection violations.

### 6.2.1.11. Greece

In response to a complaint, the Hellenic SA conducted an investigation regarding the lawfulness of personal data processing on a server of the company ALLSEAS MARINE S.A. Specifically, the Hellenic SA investigation covered access

to and inspection by an employer of an employee's emails on a company server; the illegal installation and operation of a closed-circuit video-surveillance system; and infringement of the right of access. The Hellenic SA found that the company had a legal right under Art. 5(1) and Art. 6(1)(f) GDPR to carry out an internal investigation that involved searching and retrieving the employee's emails. It found, however, that the closed-circuit video-surveillance system had been installed and operated illegally and, in addition, the recorded material submitted to the Hellenic SA was considered illegal. Finally, the Hellenic SA concluded that the company did not satisfy the employee's right of access to his personal data contained in his corporate PC.

Furthermore, following a complaint to the Hellenic SA that Public Power Corporation S.A. (PPC) did not satisfy the data subject's right of access to information, the Hellenic SA issued an administrative fine of EUR 5,000 to the company. One month after receiving the request, PPC, as a data controller, did not provide a response to the complainant regarding the inability to immediately meet this right. Given the recurrence of a previous similar infringement by PPC, the Hellenic SA unanimously decided that an effective, proportionate and dissuasive administrative fine should be imposed.

In another case, the Hellenic SA examined a complaint against a special education centre for its failure to satisfy the right of access exercised by a father, on behalf of his child, in the exercise of parental responsibility. The controller had not complied with the Hellenic SA's initial request to immediately satisfy the applicant's right of access. The Hellenic SA issued an order to the controller to provide the requested documents to the complainant, including tax documents. It also imposed an administrative fine of EUR 3,000 on the controller for not satisfying this right.

### 6.2.1.12. Hungary

The Hungarian SA issued many fines during 2020. This section includes some examples of key cases.

On 28 May, the Hungarian SA issued a fine of HUF 100,000,000 to a telecommunications service provider for multiple GDPR infringements. The Hungarian SA initiated an investigation following a personal data breach of which the company notified the Hungarian SA within the 72-hour period set out by the GDPR. The incident was triggered by the unauthorised access to the company's database, which had been conducted and reported in good faith by an ethical hacker. The Hungarian SA established that the company infringed provisions in Art. 5 GDPR, pertaining to purpose limitation and storage limitation, by failing to erase a test database.

In July, the Hungarian SA imposed a total of HUF 4,500,000 in data protection fines on Mediarey Hungary Services Zrt., the publisher of the Hungarian Forbes magazine, in two cases. The fines pertained to the magazine failing to carry out a proper interest assessment. It also did not inform various data subjects, who appeared in a list of the 50 richest Hungarians, of the results of comparing its own legitimate interests with that of a third party (the public) and of the data subjects themselves. Forbes also failed to provide information to the data subjects about the circumstances of the data processing and their data subject rights.

On 3 September, a company distributing shoes was fined a total amount of HUF 20,000,000. The involved data subject alleged that he received the wrong change when buying a pair of shoes and requested that the company let him see the shop's video footage of the exchange, which they did not allow without a police warrant; the company eventually deleted the footage after the retention period expired. The company failed to give its reasons for not letting him view the recordings and refused to let him exercise his rights to access and the right to restrict processing.

### 6.2.1.13. Iceland

On 5 March, the Icelandic SA decided to impose an administrative fine of ISK 3,000,000 on the National Centre of Addiction Medicine (NCAM) in a case relating to a personal data breach. The breach occurred when a former employee of the NCAM received boxes containing what were supposed to be personal belongings that he had left there. It turned out, however, that the boxes also contained patient data, including health records of 252 former patients and records containing the names of approximately 3,000 people who had attended rehabilitation for alcohol and substance abuse. The Icelandic SA concluded that the breach was a result of the data controller's lack of implementation of appropriate data protection policies and appropriate technical and organisational measures to protect the data, which constituted a violation of the GDPR, so issued the fine.

In a similar case, also on 5 March, the Icelandic SA decided to impose an administrative fine of ISK 1,300,000 on the Breiðholt Upper Secondary School pertaining to a personal data breach. The breach occurred when a teacher at the school sent an e-mail to his students and their parents/guardians, attaching a document that he believed to contain information on consultation appointments. However, it contained data on the well-being, study performance and social conditions of a different group of students; some of the personal data was sensitive. The Icelandic SA concluded that the breach resulted from a lack of implementation of appropriate data protection policies and appropriate technical and organisational measures. As such, this amounted to a violation of the GDPR and warranted the fine.

### 6.2.1.14. Ireland

On 15 December, the Irish SA announced the conclusion of a GDPR investigation it had conducted into Twitter International

Company (TIC). The Irish SA started its investigation in January 2019 following receipt of a breach notification from TIC. The Irish SA found that TIC had infringed Arts. 33(1) and 33(5) GDPR in failing to notify the Irish SA of the breach on time and failing to adequately document the breach. The Irish SA imposed an administrative fine of EUR 450,000 on TIC as an effective, proportionate and dissuasive measure.

The draft decision in this inquiry, having been submitted to other CSAs under Art. 60 GDPR in May, was the first one to go through the Art. 65 GDPR (dispute resolution) process since the introduction of the GDPR and was the first Draft Decision in a "big tech" case on which all EEA SAs were consulted as CSAs.

The EDPB has published the Art. 65 GDPR [decision](#) and the [final Irish SA decision](#) on its website.

### 6.2.1.15. Italy

The Italian SA imposed two fines on Eni Gas and Luce (Egl), totalling EUR 11,500,000, concerning respectively the illicit processing of personal data in the context of promotional activities and the activation of unsolicited contracts. The fines were determined in view of the parameters set out in the GDPR, including the wide range of stakeholders involved, the pervasiveness of the conduct, the duration of the infringement, and the economic conditions of Egl. The first fine of EUR 8,500,000 related to unlawful processing in connection with telemarketing and teleselling activities. The second fine of EUR 3,000,000 concerned breaches due to the conclusion of unsolicited contracts for the supply of electricity and gas under free market conditions.

The Italian SA fined TIM SpA (TIM) EUR 27,802,496 on account of several instances of unlawful processing for marketing purposes. Overall, the infringements concerned millions of individuals. TIM were proven to be insufficiently familiar



with fundamental features of the processing activities they performed, thus threatening accountability. In many cases out of the millions of marketing calls that had been placed in a six-month period with non-customers, the Italian SA could establish that the call centre operators relied upon by TIM had contacted the data subjects in the absence of any consent. Inaccurate, unclear data processing information was provided in connection with certain apps targeted at customers and the arrangements for obtaining the required consent were inadequate. The data breach management system also proved ineffective, and no adequate implementation and management systems were in place regarding personal data processing, which fell short of privacy by design requirements. As well as the fine, the Italian SA imposed 20 corrective measures on TIM, including both prohibitions and injunctions.

On 9 July, the Italian SA fined the telephone operators Wind Tre SpA and Iliad about EUR 17,000,000 and EUR 800,000, respectively. The Wind Tre SpA fine was issued on account of several instances of unlawful data processing that were mostly related to unsolicited marketing communications made without users' consent. Some users had been unable to withdraw consent or object to the processing of their personal data for marketing processes. The Italian SA had already issued a prohibitory injunction against the company on account of similar infringements that had occurred when the previous data protection law was in force. The other telephone operator, Iliad, had shown shortcomings in particular concerning employees' access to traffic data.

The Italian SA ordered Vodafone to pay a fine of more than EUR 12,250,000 on account of having unlawfully processed the personal data of millions of users for telemarketing purposes. As well as having to pay the fine, the company was required to implement several measures set out by the Italian SA to comply with national and EU data protection legislation.

Furthermore, pertaining to the private sector, the Italian SA made two decisions providing for corrective measures and administrative fines. Related to the public sector, the Italian SA issued 20 reprimands and 30 administrative fines without corrective measures. Significant cases involved municipalities, universities, health care organisations and schools.

### 6.2.1.16. Latvia

The Latvian SA imposed a fine of EUR 15,000 on one of the biggest online stores in Latvia (SIA "HH Invest"). The Latvian SA examined the content of the website's privacy policy, concluding that the information available to data subjects was not in easy-to-understand language and that information was provided in a non-systematic way. Furthermore, it was established that certain aspects of the processing that had to be explained to the data subject in accordance with Art. 13 GDPR were not clarified. The administrative fine was imposed taking into account the fact that the online store actively cooperated with the Latvian SA during the inspection and had remedied the non-compliance identified by the Latvian SA.

The Latvian SA also imposed a fine of EUR 6,250 on a company for the improper processing of employee personal data. The Latvian SA received a complaint about the actions of the employer in sending third persons (other employees) an e-mail containing information about the data subjects' names and health conditions, including diagnoses of infectious disease. After investigation, the Latvian SA found that the relevant personal data had been processed inappropriately because such processing was not necessary to achieve the employer's objectives and no legal basis under Art. 9 GDPR was applicable to such processing. When imposing a fine, the Latvian SA considered that the incident was an isolated incident and that no evidence was found that the company would do this systematically.

### 6.2.1.17. Lithuania

In 2020, the Lithuanian SA imposed multiple fines for GDPR violations. Most of the fines were imposed because of non-cooperation, where the organisations involved in the investigation did not provide the requested information to the Lithuanian SA.

In April, the Lithuanian SA carried out an investigation into sound recording in public transport buses. The Lithuanian SA fined the private company UAB "Vilniaus viešasis transportas" EUR 8,000 for violating Arts. 5, 13, 24 and 35 GDPR.

In September, the Lithuanian SA reprimanded the Vilnius City Municipality Administration for infringements of Arts. 5(1)(d) and 5(1)(f) GDPR. Specifically, the Municipality Administration had failed to implement appropriate technical and organisational measures, thereby failing to ensure the accuracy of personal data pertaining to the parents of an adopted child. The Lithuanian SA fined the Municipality Administration EUR 15,000.

### 6.2.1.18. The Netherlands

The Dutch SA imposed seven fines in 2020. Not all these fines have been made public, so the Dutch SA may not yet disclose the amount of the fines and other details. In addition to these fines, the Dutch SA issued one order subject to penalty and took a number of other corrective measures. Some cases are listed here:

- In February, the Dutch SA published an order subject to penalty directed at health insurance company CZ because the company processed too much medical data for the assessment of applications for reimbursement of rehabilitation care;
- In March, the Dutch SA fined the tennis association KNLTB EUR 525,000 for selling the personal data of its members;
- In April, the Dutch SA published a fine of EUR 725,000,

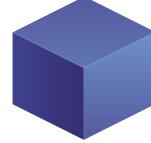
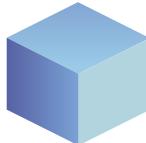
imposed on a company that required employees to have their fingerprints scanned for time and attendance registration. Following an investigation, the Dutch SA concluded that the company was not authorised to process its employees' fingerprint data. The company was not entitled to invoke an exemption for processing sensitive personal data;

- In July, the Dutch SA imposed a fine of EUR 830,000 on the National Credit Register (BKR). The BKR had created too many obstacles for people wishing to access their data. Among other things, the BKR charged people who wished access to the personal data that the BKR had about them.

### 6.2.1.19. Norway

The Norwegian SA issued multiple fines in 2020. The Norwegian SA carried out the following actions:

- Imposed an administrative fine equivalent to EUR 18,870 on the Indre Østfold Municipality due to a breach of confidentiality, where personal data that should have been protected was made available to unauthorised persons;
- Reprimanded Telenor Norge AS for a lack of personal data security in a voice mailbox function, and for failing to notify the Norwegian SA of a data breach;
- Notified the Norwegian Institute of Public Health (NIPH) of its intention to impose a temporary ban on personal data processing in connection with the Smittestopp contact tracing mobile app. The NIPH temporarily suspended all use of the app. In August, the Norwegian SA reached a decision to temporarily ban the processing of personal data using the Smittestopp app as it could not be considered a proportionate intervention in a user's fundamental right to data protection. The NIPH had already decided to stop collecting personal data and to erase the collected data;
- Imposed an administrative fine equivalent to EUR 47,500 on the Rælingen Municipality after data concerning the health of children with special needs was processed using the digital learning platform Showbie;



- Issued the Norwegian Public Roads Administration a fine equivalent to EUR 37,400 for processing personal data for purposes that were incompatible with the originally stated purposes, and for not erasing video recordings after seven days;
- Made final a decision to issue an administrative fine to the Bergen Municipality equivalent to approximately EUR 276,000. This was in response to a data breach in October 2019 regarding the Municipality's new tool for communication between school and home. Personal information in the communication system was not secure enough;
- Issued Odin Flisenter AS with an administrative fine equivalent to EUR 13,905 for performing a credit check of a sole proprietorship without having a lawful basis for the processing;
- Decided on an administrative fee of NOK 750,000 for the Østfold HF Hospital. During the period from 2013 to 2019, the hospital stored report extracts from patient records that were not access controlled, so were stored in a non-secure manner. The case started with a personal data breach notification from the hospital. The Norwegian SA considered that the Østfold HF Hospital had not established a system for access control that was sufficient to prevent similar breaches from occurring in the future, and referred particularly to the routines for access control and personal data storage. The management system was required to involve follow-up that the routines are followed, which also means ensuring that only secure systems are used in the processing of sensitive personal data.

### 6.2.1.20. Poland

The President of the Polish SA imposed 11 administrative fines in 2020, some of which are listed below:

- On 18 February, the Polish SA imposed a fine of PLN 20,000 (EUR 4,600) in connection with a breach consisting of the processing of the biometric data of children when using the school canteen without a legal basis;

- On 9 March, the Polish SA imposed a fine of PLN 20,000 (EUR 4,600) on Vis Consulting Sp. z o.o., a company from the telemarketing industry, for making it impossible to conduct an inspection;
- On 29 May, the Polish SA imposed a fine of PLN 15,000 (EUR 3,500) in cross-border proceedings on the East Power company from Jelenia Góra for failing to provide the Polish SA with access to personal data and other information necessary for the performance of its tasks;
- On 3 June, the Polish SA imposed a fine of PLN 5,000 (EUR 1,168) on an individual entrepreneur running a non-public nursery and pre-school for failing to provide the Polish SA with access to personal data and other information necessary for the performance of its tasks;
- On 2 July, the Polish SA imposed a fine of PLN 100,000 (EUR 23,000) on the Surveyor General of Poland for failing to provide the Polish SA with access to premises, data processing equipment and means, and access to personal data and information necessary for the Polish SA to perform its tasks during the inspection;
- In addition, on 24 August, the Polish SA imposed another fine of PLN 100,000 (EUR 23,000) on the Surveyor General of Poland for infringing the principle of lawfulness of personal data processing;
- On 21 August, the Polish SA imposed a fine on the Warsaw University of Life Sciences of PLN 50,000 (EUR 11,500) after having found a personal data breach;
- On 3 December, the Polish SA imposed a fine of PLN 1,900,000 million (EUR 460,000) on Virgin Mobile Polska for not implementing appropriate technical and organisational measures to ensure the security of the processed data;
- On 9 December, the Polish SA imposed a fine of over PLN 12,000 (EUR 3,000) on a Smart Cities company from Warsaw for not cooperating with the Polish SA;
- On 9 December, the Polish SA imposed a fine of PLN 85,588 (EUR 20,000) on WARTA S.A. Insurance and Reinsurance Company for failing to notify the President of the Polish SA of a personal data breach;

- On 17 December, the Polish SA imposed a fine of over PLN 1,000,000 (EUR 250,000) on the ID Finance Poland company for failing to implement appropriate technical and organizational measures.

### 6.2.1.21. Portugal

The Portuguese SA issued several corrective measures within its powers under Art. 58 GDPR. In one example, it compelled a controller in the field of market studies to delete a data subject's personal data.

In two cases, the Portuguese SA ordered two controllers and one processor, all in the public health sector, to bring data processing into compliance with the GDPR and to adopt specific measures to remedy the deficiencies found within the context of COVID-19 data processing. There were also two situations where the Portuguese SA issued an order to temporarily ban data processing until certain conditions were met. Both cases related to the collection by web cameras of images of people on the beach, which were transmitted online in real-time. The two different private data controllers had to take the appropriate technical measures to process images with no identifiable individuals.

The Portuguese SA also imposed a fine on a private company for violating the principle of lawfulness. Due to the COVID-19 pandemic, all sanction proceedings were suspended for four months, in accordance with national law. Therefore, although some proceedings were ongoing and controllers were already notified of a draft decision involving the application of fines, there were no more final decisions in 2020 regarding GDPR cases; they only pertained to ePrivacy cases.

### 6.2.1.22. Romania

In 2020, the Romanian SA conducted 21 enforcement measures for violations of the GDPR, as outlined here.

- On 13 January, the Romanian SA fined Hora Credit IFN S.A. the equivalent of EUR 14,000 for multiple GDPR violations and issued various corrective measures to ensure compliance with the GDPR;
- On 14 January, the Romanian SA sanctioned SC Enel Energie S.A with two fines amounting to the equivalent of EUR 6,000 for violating provisions within Arts. 5, 6, 7 and 21 GDPR;
- On 25 March, the Romanian SA imposed several administrative fines and corrective measures on three data controllers. The controller Dante Internațional SA was sanctioned with an administrative fine of the equivalent of EUR 3,000; the controller Association "SOS Infertilitatea" with the equivalent of EUR 2,000; and the controller Vodafone România SA with the equivalent of EUR 4,100;
- On 31 March, the Romanian SA fined Vodafone România the equivalent of EUR 3,000 for violating Art. 5 GDPR and imposed corrective measures to ensure its compliance with the GDPR;
- On 11 June, the Romanian SA imposed two fines: controller Estee Lauder Romania SRL was sanctioned with a fine equivalent to EUR 3,000 for unlawful data processing and the controller Telekom Romania Communications SA was fined the equivalent of EUR 3,000 for not implementing sufficient security measures;
- On 18 June, the Romanian SA found that Enel Energie Muntenia SA did not implement sufficient security and confidentiality measures to prevent the accidental disclosure of personal data to unauthorised persons and fined them the equivalent of EUR 4,000;
- On 9 July, the Romanian SA found that Proleasing Motors SRL had violated Art. 32 GDPR and subsequently fined them the equivalent of EUR 15,000;
- On 27 July, the Romanian SA fined SC CNTAR TAROM SA the equivalent of EUR 5,000 and imposed a corrective measure to ensure the controller reviewed and updated the technical and organisational measures it had in place;

- On 30 July, the Romanian SA imposed two fines. First, it fined S.C. Viva Credit IFN S.A. the equivalent of EUR 2,000 and imposed corrective measures. Second, it fined controller Compania Națională Poșta Română the equivalent of EUR 2,000;
- On 1 September, the Romanian SA sanctioned the Owners' Association Block FC 5, Năvodari city, Constanța county with a fine equivalent to EUR 500; it reprimanded the Owners' Association for failing to adhere to certain provisions in the GDPR; and imposed certain corrective measures;
- On 8 September, the controller Sanatatea Press Group S.R.L. was sanctioned with a fine equivalent to EUR 2,000 for not adhering to data security measures;
- On 1 October, the Romanian SA fined Megareduceri TV S.R.L. the equivalent of EUR 3,000 and fined the Owners' Association Militari R, Chiajna village the equivalent of EUR 2,000 and imposed a corrective measure;
- On 15 October, the controller S.C. Marsorom S.R.L. was sanctioned with a fine equivalent to EUR 3,000;
- On 20 October, the Romanian SA fined controller Globus Score SRL the equivalent of EUR 2,000 for failing to fulfil an earlier corrective measure and imposed another corrective measure;
- On 23 November, the Romanian SA fined Vodafone România S.A. the equivalent of EUR 4,000 for not responding to data subject access and erasure requests, and issued a corrective measure;
- On 24 November, the Romanian SA issued a fine equivalent to EUR 5,000 to DADA CREATION S.R.L. for violating Art. 32 GDPR and reprimanded the controller for infringing Art. 33 GDPR. The Romanian SA also issued a corrective measure.

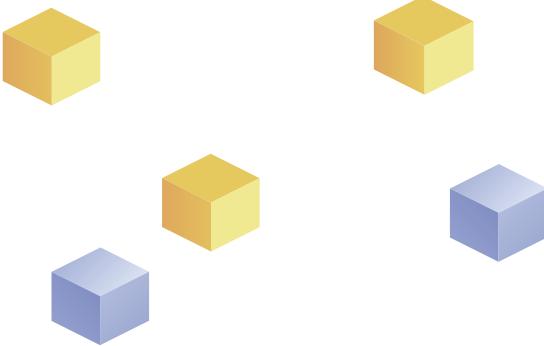
### 6.2.1.23. Slovakia

The Slovak SA fined a primary school EUR 6,000 for breaching the principle of lawfulness, principle of accountability and for the failure to comply with its obligation to handle the data subjects' requests to an adequate extent.

### 6.2.1.24. Slovenia

The Slovenian SA often deals with cases regarding unlawful video surveillance in work areas. There are some specific provisions on video surveillance permissibility in national law, in addition to the GDPR provisions. In one such case, the Slovenian SA did not permit video surveillance as a means for an employer to constantly monitor the work process by using an app on his mobile phone. According to national law, video surveillance within work areas may only be implemented in exceptional cases when it is necessarily required for the safety of people or property, or to protect secret data and business secrets.

An individual exercised his right to rectification regarding his financial information in SISBON, which is a Slovenian information system on credit ratings that is designed for mutual exchange and processing of data on natural persons. The Bank of Slovenia manages SISBON, and all the banks and most of the financial subjects are required to provide information to the system. The individual's demand to rectify the information had been denied by the data controller (bank). Later, the primary bank was no longer technically able to rectify the data for the subject. The new creditor was not a member of SISBON and could not rectify the data. The Slovenian SA decided that the data controller violated the individual's right to rectification under the GDPR and that technical rules on managing the system should enable individuals to exercise this right.



A parish was processing the application of an individual on the right of erasure. The individual requested his personal data be erased from the register of births because he was no longer a member of the church. The Slovenian SA agreed with the position of the church, confirming that the register is an archive document, and the individual may not claim the right to erasure when the processing is needed for archiving purposes in the public interest.

The national health insurance fund was sending professional cards to users by mail and with personal data printed on the envelope (the insurance number, the barcode and the summary of the consignment). The Slovenian SA ordered the data processor to restrict the listing of the personal data on the envelope.

### 6.2.1.25. Spain

The Spanish SA fined the company Iberdrola EUR 4,000 for not responding to its request for information. In short, Iberdrola had not provided the information required and consequently hindered the investigative powers that each Spanish SA has, thereby infringing Art. 58(1) GDPR.

The Spanish SA issued a fine of EUR 1,200 to a company for calling the data subject and offering him/her a deal on hotels, while he/she was in an advertisement exclusion system. By joining this system, the data subject had exercised his/her right to object to processing for marketing purposes under Art. 21 GDPR. The company, however, did not comply with its obligation to consult the advertisement exclusion system before making a telephone call with marketing purposes to avoid processing certain individuals' personal data.

The Spanish SA also fined Vodafone España EUR 75,000 for processing a claimant's telephone number for marketing purposes after the claimant had exercised the right to erasure in 2015, in spite of which the data subject was sent advertising

messages. The controller stated that the claimant number, being easy to remember, had been used as a "dummy number" by its employees.

The Spanish SA imposed also a fine of EUR 70,000 on Xfera Móviles for disclosing a customer's personal data to a third party. The SA issued a fine of EUR 75,000 to Telefónica Móviles España, S.A.U. for unlawfully processing a claimant's personal data by charging the claimant several invoices corresponding to a third person.

#### 6.2.1.26. Sweden

The Swedish SA issued multiple fines in 2020. The Swedish SA carried out these enforcement acts:

- Imposed an administrative fine of SEK 75,000,000 on Google for failing to comply with the GDPR. As a search engine operator, it had not fulfilled its obligations in respect to the right to request delisting;
- Issued a fine of SEK 200,000 to the National Government Service Centre for failing to notify affected parties as well as the Swedish SA about a personal data breach in due time;
- In response to a complaint, conducted an investigation that showed that the Healthcare Committee in Region Örebro County made a mistake when publishing sensitive personal data about a patient admitted to a forensic psychiatric clinic on the region's website. The Swedish SA ordered the Committee to bring its personal data handling into compliance with the GDPR and furthermore issued an administrative fine of SEK 120,000 against the Committee;
- Investigated the use by a co-operative housing association of video surveillance on its property. It concluded that the association had gone too far when using video surveillance in the main entrance and stairwell, and when recording audio. The Swedish SA ordered the co-operative housing association to stop these specific surveillance activities and to improve the information provided concerning the video surveillance. Furthermore, it issued an administrative

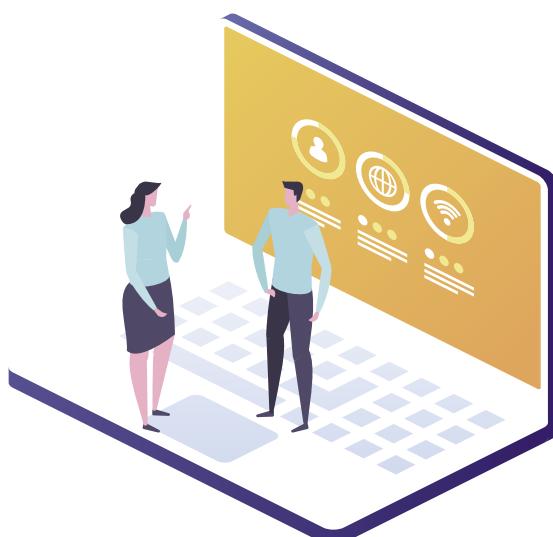
fine of SEK 20,000 to the association. When calculating the amount of the fine, the Swedish SA considered the fact that it was a smaller co-operative housing association;

- Reviewed the so-called School Platform, which is the IT system used, among other things, for student administration of schools in the City of Stockholm. The review showed an insufficient level of security of such a grave nature that the Swedish SA issued an administrative fine of SEK 4,000,000 to the Board of Education in the City of Stockholm;
- Received a complaint from the relative of a resident of a residential care home for persons with certain functional impairments (so-called LSS housing) in Gnosjö Municipality, claiming that the resident was being monitored illegally. The Swedish SA initiated an audit of the LSS housing and concluded that the resident in question was indeed monitored in his/her bedroom in violation of the GDPR and the Swedish Video Surveillance Act. In its decision, the Swedish SA stated that there was no legal basis for the video surveillance, that an Impact Assessment had not been carried out before initiating the video surveillance and that the controller had failed to clearly inform the resident about the video surveillance. For these reasons, the Swedish SA issued an administrative fine of SEK 200,000 to the Social Welfare Committee;
- Audited eight health care providers in how they governed and restricted personnel's access to the main systems for electronic health records. The Swedish SA discovered insufficiencies that in seven of the eight cases lead to administrative fines of up to SEK 30,000,000;
- Issued a fine of SEK 550,000 against the Umeå University for failing to sufficiently protect sensitive personal data. Specifically, the University had processed special categories of personal data concerning sexual life and health through, amongst others, storage on a cloud service, without sufficiently protecting the data;
- Imposed an administrative fine of SEK 300,000 on a housing company for unlawful video surveillance in an apartment building.

### 6.3. SURVEY – BUDGET AND STAFF

In the context of the evaluation of the GDPR, the EDPB conducted a survey among the SAs about their budget and staff. Based on information provided by SAs from 30 EEA countries before February 2020, an increase in the budget for 2020 was envisaged in 26 cases. In respect of the remaining four SAs, three forecasted no change and for one no data was available. According to the same survey, a majority of SAs (23) anticipated an increase in staff numbers in 2020. Five SAs forecast that the number of their employees would not increase from 2019 to 2020, while two SAs predicted a decrease in staff numbers. Differences in personnel requirements across SAs are to be expected, given the varied remits of the SAs.

In its contribution to the evaluation of the GDPR, the EDPB stresses that the effective application of the powers and tasks attributed by the GDPR to SAs is largely dependent on the resources available to them. Even though most SAs reported an increase in staff and resources, a majority of the SAs stated that resources made available to them were insufficient. The EDPB noted that this applies, in particular, to the OSS mechanism, as its success depends on the time and effort that SAs can dedicate to individual cases and cooperation.



# 7



## Coordinated Supervision Committee of the large EU Information Systems and of EU bodies, offices and agencies

In accordance with Art. 62 of Regulation 2018/1725, the European Data Protection Supervisor (EDPS) and the national Supervisory Authorities (SAs) shall cooperate actively to ensure effective supervision of large-scale IT systems and of EU bodies, offices and agencies. For this purpose, the EDPS and SAs shall meet at least twice per year within the framework of the EDPB. Additionally, several legal acts on large-scale IT systems and EU agencies refer to this model of coordinated supervision.

To ensure the consistency of supervision efforts on both levels, all SAs involved, including the EDPS, used to cooperate through Supervision Coordination Groups (SCGs). Each of these groups was dedicated to a specific EU database.

Since December 2018, Regulation 2018/1725 has provided for a single model of coordinated supervision for large-scale EU IT systems and agencies within the framework of the EDPB. This replaces the current system of individual SCGs. The new model does not apply to all EU information systems and agencies at once, but progressively, according to when the revised version of the establishing act of each EU information system and agency becomes applicable.

In December 2019, the Coordinated Supervision Committee (CSC) was formally established within the EDPB. It brings together the SAs of each EU Member State and the EDPS, as well as SAs of non-EU Members of the Schengen Area when foreseen under EU law.

The CSC's tasks include, among others, supporting SAs in carrying out audits and inspections; working on the interpretation or application of the relevant EU legal act; studying problems within the exercise of independent supervision or within the exercise of data subject rights; drawing up harmonised proposals for solutions; and promoting awareness of data protection rights.

Participation in the CSC meetings can occur under various arrangements, depending on the IT system, body, office or agency for which supervision is taking place, as well as the respective EU legal act. As announced in December 2020, during its third plenary meeting, the CSC elected Clara Guerra from the Portuguese SA to succeed Giuseppe Busia as its new Coordinator for a term of two years. Iris Gnedler from the German Federal SA will stay on as Deputy Coordinator for another year.

Pursuant to Art. 62 of Regulation 2018/1725, the following EU large-scale IT systems, bodies, offices and agencies currently fall under the CSC's scope:

#### **Internal Market:**

- Internal Market Information System (IMI), which allows the exchange of information between public authorities involved in the practical implementation of EU law.

#### **Police and Judicial Cooperation:**

- Eurojust, the agency responsible for judicial cooperation in criminal matters among EU Member States.

In the future, all coordinated supervision of large EU information systems, bodies, offices and agencies will gradually be moved to the CSC, including:

#### **Border, Asylum and Migration:**

- Schengen Information System (SIS), ensuring border control cooperation (before the end of 2021);
- Entry Exit System (EES), which registers entry and exit

data and refusal of entry data of third country nationals crossing the external borders of the Schengen States (expected in 2022);

- European Travel Information and Authorisation System (ETIAS), which tracks visitors from countries who do not need a visa to enter the Schengen Zone (expected in 2022);
- Visa Information System (VIS), connecting consulates in non-EU countries and all external border-crossing points of Schengen States (expected in 2023);
- Eurodac, which compares fingerprints of asylum applicants to see if they have previously applied for asylum or entered the EU irregularly via another Member State;
- Customs Information System (CIS), which is an automated information system that assists EU State administrative authorities in preventing, investigating and prosecuting operations that are in breach of customs or agricultural legislation.

#### **Police and Judicial Cooperation:**

- SIS, which also ensures law enforcement cooperation (before the end of 2021);
- European Public Prosecutor Office (EPPO) (before the end of 2021);
- European Criminal Records Information System on third country nationals (ECRIS-TCN), which allows EU Member State authorities to identify which other Member States hold criminal records on third country nationals or stateless persons being checked (expected for 2022);
- Europol, the EU's law enforcement agency (expected by end of 2021 or early 2022).

# 8



## Main objectives for 2021

In early 2021, the EDPB adopted its two-year work programme for 2021-2022, according to Art. 29 of the EDPB Rules of Procedure. The work programme follows the priorities set out in the EDPB 2021-2023 Strategy and will put the EDPB's strategic objectives into practice.

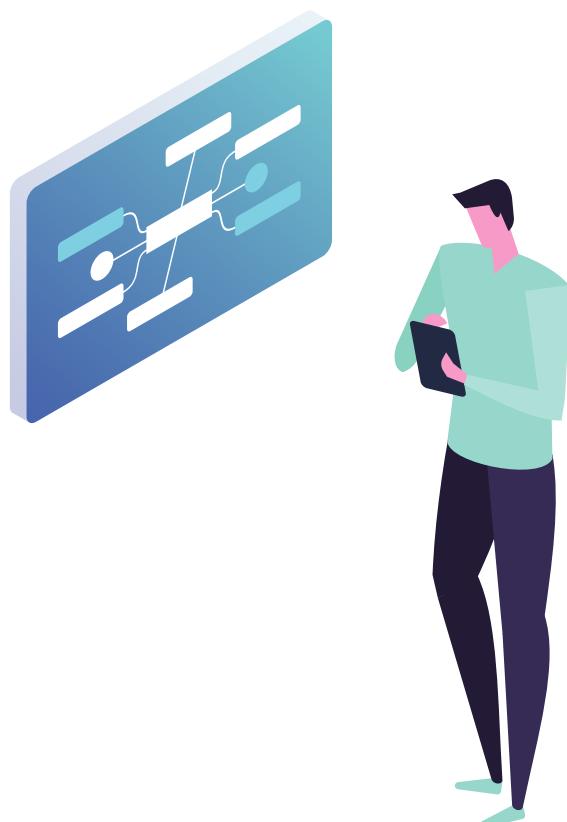
### 8.1. 2021-2023 STRATEGY

The EDPB defined its [Strategy for 2021-2023](#), which covers the four main pillars of its strategic objectives, as well as a set of three key actions per pillar to help achieve these objectives.

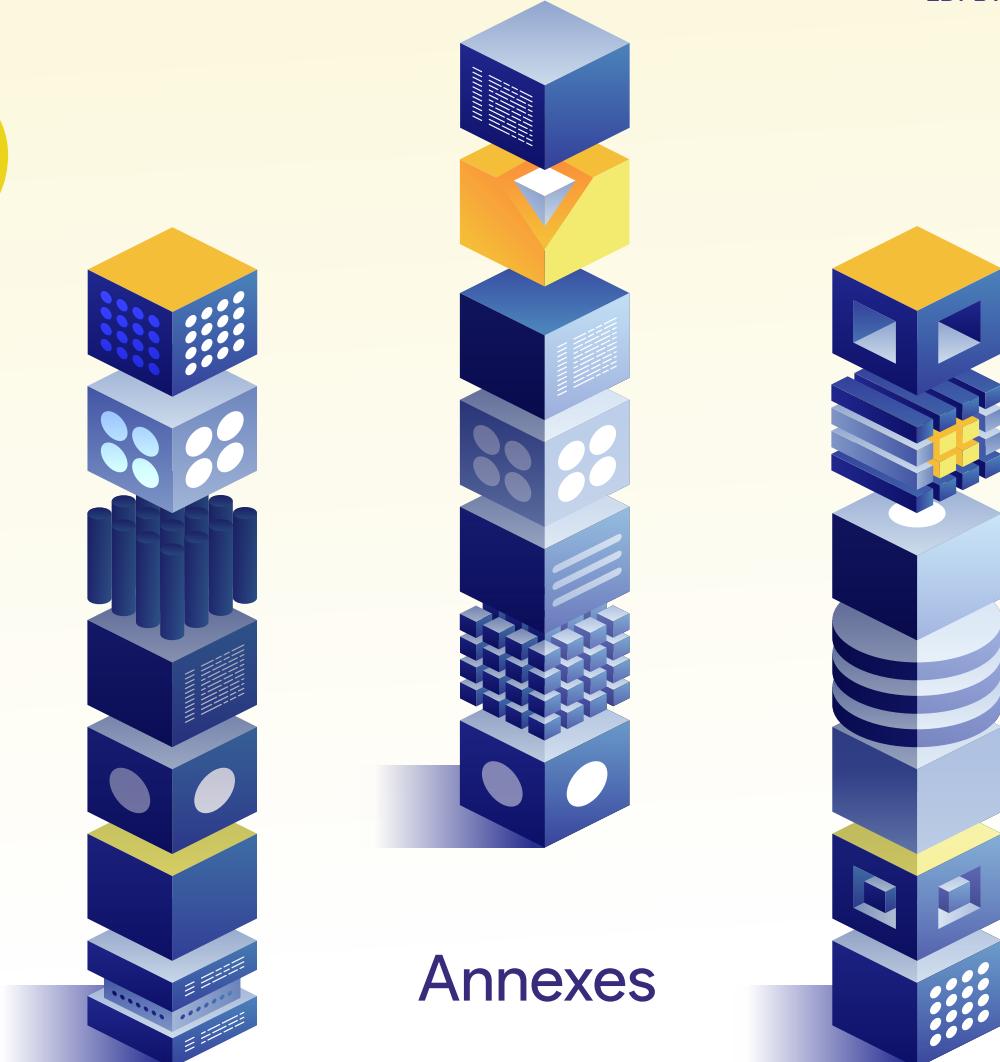
The pillars and key actions are as follows:

- 1. Advancing harmonisation and facilitating compliance by:**
  - a.** Providing guidance on key notions of EU data protection law;
  - b.** Promoting development and implementation of compliance mechanisms for data controllers and processors;
  - c.** Fostering the development of common tools for a wider audience and engaging in awareness raising and outreach activities.

2. Supporting **effective enforcement** and **efficient cooperation between national SAs** by:
  - a. Encouraging and facilitating use of the full range of cooperation tools enshrined in Chapter VII GDPR and Chapter VII Law Enforcement Directive;
  - b. Implementing a Coordinated Enforcement Framework (CEF) to facilitate joint actions;
  - c. Establishing a Support Pool of Experts (SPE).
3. Promoting a **fundamental rights approach to new technologies** by:
  - a. Assessing those technologies;
  - b. Reinforcing data protection by design and by default and accountability;
  - c. Intensifying engagement and cooperation with other regulators and policymakers.
4. Advancing a **global dimension** by:
  - a. Promoting and increasing awareness of the use and implementation of transfer tools which ensure a level of protection equivalent to the EEA;
  - b. Engaging with the international community;
  - c. Facilitating the engagement between the EDPB Members and the SAs of third countries with a focus on cooperation in enforcement cases involving controllers or processors located outside the EEA.



# 9



## 9.1. GENERAL GUIDANCE ADOPTED IN 2020

- Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications
- Guidelines 02/2020 on Arts. 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
- Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak
- Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak
- Guidelines 05/2020 on consent under Regulation 2016/679

- Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR - Adopted after public consultation
- Guidelines 07/2020 on the concepts of controller and processor in the GDPR
- Guidelines 08/2020 on the targeting of social media users
- Guidelines 09/2020 on relevant and reasoned objection under Regulation 2016/679
- Guidelines 10/2020 on restrictions under Art. 23 GDPR
- Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data - version for public consultation
- Recommendations 02/2020 on the European Essential Guarantees for surveillance measures

## 9.2. CONSISTENCY OPINIONS ADOPTED IN 2020

- Opinion 01/2020 on the Spanish data protection Supervisory Authority draft accreditation requirements for a code of conduct monitoring body pursuant to Art. 41 GDPR
- Opinion 02/2020 on the Belgium data protection Supervisory Authority draft accreditation requirements for a code of conduct monitoring body pursuant to Art. 41 GDPR
- Opinion 03/2020 on the France data protection Supervisory Authority draft accreditation requirements for a code of conduct monitoring body pursuant to Art. 41 GDPR
- Opinion 04/2020 on the draft decision of the competent Supervisory Authority of the United Kingdom regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR
- Opinion 05/2020 on the draft decision of the competent Supervisory Authority of Luxembourg regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR
- Opinion 06/2020 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of Fujikura Automotive Europe Group (FAE Group)
- Opinion 07/2020 on the draft list of the competent Supervisory Authority of France regarding the processing operations exempt from the requirement of a data protection impact assessment (Art. 35(5) GDPR)
- Opinion 08/2020 on the draft decision of the Irish Supervisory Authority regarding the Controller Binding Corporate Rules of Reinsurance Group of America
- Opinion 09/2020 on the draft decision of the Irish Supervisory Authority regarding the Processor Binding Corporate Rules of Reinsurance Group of America
- Opinion 10/2020 on the draft decision of the competent Supervisory Authorities of Germany regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR
- Opinion 11/2020 on the draft decision of the competent Supervisory Authority of Ireland regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR
- Opinion 12/2020 on the draft decision of the competent Supervisory Authority of Finland regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR
- Opinion 13/2020 on the draft decision of the competent Supervisory Authority of Italy regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR
- Opinion 14/2020 on the draft decision of the competent Supervisory Authority of Ireland regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR
- Opinion 15/2020 on the draft decision of the competent Supervisory Authorities of Germany regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR
- Opinion 16/2020 on the draft decision of the competent Supervisory Authority of the Czech Republic regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR
- Opinion 17/2020 on the draft Standard Contractual Clauses submitted by the Slovenian Supervisory Authority (Art. 28(8) GDPR)
- Opinion 18/2020 on the draft decision of the competent Supervisory Authority of the Netherlands regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR

- Opinion 19/2020 on the draft decision of the competent Supervisory Authority of Denmark regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR
- Opinion 20/2020 on the draft decision of the competent Supervisory Authority of Greece regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR
- Opinion 21/2020 on the draft decision of the competent Supervisory Authority of the Netherlands regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR
- Opinion 22/2020 on the draft decision of the competent Supervisory Authority of Greece regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR
- Opinion 23/2020 on the draft decision of the competent supervisory authority of Italy regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR
- Opinion 24/2020 on the draft decision of the Norwegian Supervisory Authority regarding the Controller Binding Corporate Rules of Jotun
- Opinion 25/2020 on the draft decision of the Swedish Supervisory Authority regarding the Controller Binding Corporate Rules of Tetra Pak
- Opinion 26/2020 on the draft decision of the competent Supervisory Authority of Denmark regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR
- Opinion 27/2020 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of Coloplast Group
- Opinion 28/2020 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of Iberdrola Group
- Opinion 29/2020 on the draft decision of the Lower Saxony Supervisory Authority regarding the Controller Binding Corporate Rules of Novelis Group
- Opinion 30/2020 on the draft decision of the competent Supervisory Authority of Austria regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR
- Opinion 31/2020 on the draft decision of the competent Supervisory Authority of Poland regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR
- Opinion 32/2020 on the draft decision of the Dutch Supervisory Authority regarding the Controller Binding Corporate Rules of Equinix

### 9.3. LEGISLATIVE CONSULTATION

- EDPB Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic – 14/04/2020
- Statement on the ePrivacy Regulation and the future role of Supervisory Authorities and the EDPB - 19/11/2020

### 9.4. OTHER DOCUMENTS

- Contribution of the EDPB to the evaluation of the GDPR under Art. 97 - 18/02/2020
  - Individual replies from the data protection supervisory authorities
- Statement on privacy implications of mergers – 19/02/2020
- Statement on the processing of personal data in the context of the COVID-19 outbreak – 19/03/2020

- Mandate on the processing of health data for research purposes in the context of the COVID-19 outbreak – 07/04/2020
- Mandate on geolocation and other tracing tools in the context of the COVID-19 outbreak – 07/04/2020
- Statement on restrictions on data subject rights in connection to the state of emergency in Member States – 02/06/2020
- Statement on the processing of personal data in the context of reopening of borders following the COVID-19 outbreak - 16/06/2020
- Statement on the data protection impact of the interoperability of contact tracing apps - 16/06/2020
- Statement on the Court of Justice of the European Union Judgment in Case C-311/18 - Data Protection Commissioner v Facebook Ireland and Maximillian Schrems - 17/07/2020
- Information note on BCRs for Groups of undertakings / enterprises which have ICO as BCR Lead SA - 22/07/2020
- Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems - 24/07/2020
- EDPB Document on Coordinated Enforcement Framework under Regulation 2016/679 - 20/10/2020
- Statement on the protection of personal data processed in relation with the prevention of money laundering and terrorist financing - 15/12/2020
- EDPB Document on Terms of Reference of the EDPB Support Pool of Experts - 15/12/2020
- Information note on data transfers under the GDPR to the United Kingdom after the transition period - 15/12/2020
  - Superseded by Information note on data transfers under the GDPR to the United Kingdom after the transition period - 13/01/2021
- Statement on the end of the Brexit transition period - 15/12/2020
  - Superseded by Statement on the end of the Brexit transition period - 13/01/2021
- Pre-GDPR BCRs overview list - 21/12/2020

## 9.5. LIST OF EXPERT SUBGROUPS WITH SCOPE OF MANDATES

NAME OF EXPERT SUBGROUP (ESG)	SCOPE OF MANDATE
<b>Borders, Travel &amp; Law Enforcement (BTLE) Expert Subgroup</b>	<ul style="list-style-type: none"> <li>● Law Enforcement Directive</li> <li>● Cross-border requests for e-evidence</li> <li>● Adequacy decisions, access to transferred data by law enforcement and national intelligence authorities in third countries (e.g. follow-up to CJEU Schrems II judgment and draft EU adequacy decisions on the UK)</li> <li>● Passenger Name Records (PNR)</li> <li>● Border controls</li> </ul>
<b>Compliance, e-Government and Health (CEH) Expert Subgroup</b>	<ul style="list-style-type: none"> <li>● Codes of conduct, certification and accreditation</li> <li>● Close cooperation on DPIA with the Technology ESG focusing on the perspective of their mandates</li> <li>● Close cooperation on privacy by design and by default with the Technology ESG focusing on the perspective of their mandates</li> <li>● Compliance with public law and eGovernment</li> <li>● Health</li> <li>● Processing of personal data for scientific research purposes</li> </ul>
<b>Cooperation Expert Subgroup</b>	<ul style="list-style-type: none"> <li>● General focus on procedures of the GDPR</li> <li>● Guidance on procedural questions</li> <li>● International mutual assistance and other cooperation tools to enforce the GDPR outside the EU (Art. 50 GDPR)</li> </ul>
<b>Coordinators Expert Subgroup</b>	<ul style="list-style-type: none"> <li>● General coordination between the Expert Subgroup Coordinators</li> <li>● Coordination on the annual Expert Subgroup working plan</li> </ul>

NAME OF EXPERT SUBGROUP (ESG)	SCOPE OF MANDATE
<b>Enforcement Expert Subgroup</b>	<ul style="list-style-type: none"> <li>● Mapping/analysing the need for additional clarifications or guidance, based on practical experiences with the application of Chapters VI, VII and VIII GDPR</li> <li>● Mapping/analysing possible updates of existing Cooperation subgroup tools</li> <li>● Monitoring of investigation activities</li> <li>● Practical questions on investigations</li> <li>● Guidance on the practical application of Chapter VII GDPR including exchanges on concrete cases</li> <li>● Guidance on the application of Chapter VIII GDPR together with the Taskforce on Administrative Fines</li> </ul>
<b>Financial Matters Expert Subgroup</b>	<p>Application of data protection principles in the financial sector (e.g. automatic exchange of personal data for tax purposes; impact of FATCA on the protection of personal data; interplay between Second Payment Services Directive and GDPR)</p>
<b>International Transfers Expert Subgroup</b>	<p>Guidance on Chapter V (International transfer tools and policy issues), more specifically:</p> <ul style="list-style-type: none"> <li>● Review European Commission Adequacy decisions</li> <li>● Guidelines on Art. 46 GDPR and review of administrative arrangements between public authorities and bodies (e.g. ESMA)</li> <li>● Codes of conduct and certification as transfer tools</li> <li>● Art. 48 GDPR together with BTLE ESG</li> <li>● Art. 50 GDPR together with Cooperation ESG</li> <li>● Guidelines on territorial scope and the interplay with Chapter V of the GDPR - interaction with Key Provisions ESG</li> <li>● Exchange of information on review of BCRs and ad hoc contractual clauses according to Art. 64 GDPR</li> </ul>

NAME OF EXPERT SUBGROUP (ESG)	SCOPE OF MANDATE
<b>IT Users Expert Subgroup</b>	<p>Developing and testing IT tools used by the EDPB with a practical focus:</p> <ul style="list-style-type: none"> <li>● Collecting feedback on the IT system from users</li> <li>● Adapting the systems and manuals</li> <li>● Discussing other business needs including tele- and videoconference systems</li> </ul>
<b>Key Provisions Expert Subgroup</b>	<p>Guidance on core concepts and principles of the GDPR, including Chapters I (e.g. scope, definitions like LSA and large-scale processing) and II (main principles); Chapters III (e.g. rights of individuals, transparency), IV (e.g. DPO – shared competences with CEH ESG, Enforcement ESG and Technology ESG) and IX</p>
<b>Social Media Expert Subgroup</b>	<ul style="list-style-type: none"> <li>● Analysing social media services, conceived as online platforms that focus on enabling the development of networks and communities of users, among which information and content is shared and whereby additional functions provided by social media services include targeting, personalisation, application integration, social plug-ins, user authentication, analytics and publishing</li> <li>● Analysing established and emerging functions offered by social media, including the underlying processing activities and corresponding risks for the rights and freedoms of individuals</li> <li>● Developing guidance, recommendations and best practices in relation to both the offer and use of social media functions, in particular for economic or political reasons</li> <li>● Providing assistance to other subgroups, in particular by proposing strategic priorities in terms of (a) supervision and (b) the development of new EDPB guidance or updating of existing WP29 guidance</li> </ul>

NAME OF EXPERT SUBGROUP (ESG)	SCOPE OF MANDATE
<b>Strategic Advisory Expert Subgroup</b>	<ul style="list-style-type: none"> <li>● Guidance on strategic questions affecting the whole EDPB (including the discussion on the work plans of the ESGs)</li> <li>● Clarification of questions that could not be resolved in the ESG</li> </ul>
<b>Taskforce on Administrative Fines</b>	Development of Guidelines on the harmonisation of the calculation of fines
<b>Technology Expert Subgroup</b>	<ul style="list-style-type: none"> <li>● Technology, innovation, information security, confidentiality of communication in general</li> <li>● ePrivacy, encryption</li> <li>● DPIA and data breach notifications</li> <li>● Emerging technologies, innovation and other challenges related to privacy: reflecting on data protection risks of future technological developments</li> <li>● Providing input on technology matters relevant to other ESG</li> <li>● Geolocation and other tracing tools in the context of the COVID-19 outbreak</li> </ul>



# Contact details

## Postal address

Rue Wiertz 60, B-1047 Brussels

## Office address

Rue Montoyer 30, B-1000 Brussels

# 2018

## ANNUAL REPORT

# COOPERATION & TRANSPARENCY



**edpb**   
European Data Protection Board

# European Data Protection Board

## 2018 Annual Report

# Cooperation & Transparency

An Executive Summary of this report, which gives an overview of key developments in EDPB activities in 2018, is also available.

Further details about EDPB can be found on our website at [edpb.europa.eu](http://edpb.europa.eu).

# TABLE OF CONTENTS

<b>1</b>	<b>2</b>	<b>3</b>
FOREWORD 4	MISSION STATEMENT, TASKS AND PRINCIPLES 5 2.1. Tasks and duties 5 2.2. Guiding principles 6	ABOUT THE EUROPEAN DATA PROTECTION BOARD 7
<b>4</b>	<b>5</b>	
2018 – AN OVERVIEW 8 4.1. Setting up the EDPB 8 4.1.1. The Rules of Procedure 8 4.1.2. Organisation of Expert Subgroups 8 4.2. Setting up the Secretariat 9 4.2.1. Memorandum of Understanding 9 4.2.2. Preparation for 25 May 2018 9 4.3. Setting up cooperation and consistency 9 4.3.1. IT communications tool (IMI) 9	EUROPEAN DATA PROTECTION BOARD ACTIVITIES IN 2018 10 5.1. General Guidance 10 5.1.1. Guidelines on certification and identifying certification criteria 11 5.1.2. Guidelines on derogations applicable to international transfers 11 5.1.3. Guidelines on territorial scope 11 5.1.4. Guidelines on accreditation 12 5.2. Consistency findings 12 5.2.1. Consistency opinions 12 5.2.2. Binding decisions 13 5.3. Legislative consultation 13 5.3.1. e-Evidence 13 5.3.2. EU-Japan draft adequacy decision 13 5.3.3. Statement on ePrivacy 14 5.4. Other documents 14 5.4.1. Letter to ICANN 14 5.4.2. Letter on the PSD2 Directive 14 5.4.3. Statement on Economic Concentration 15 5.5. Plenary meetings and subgroups 15	

**6****SUPERVISORY AUTHORITY  
ACTIVITIES IN 2018** **16**

<b>6.1. Cross-border cooperation</b>	<b>16</b>	<b>6.2.1. Some relevant national cases with exercise of corrective powers</b>	<b>20</b>
6.1.1. Preliminary procedure to identify the Lead and Concerned Supervisory Authorities	16	6.2.1.1. Austria	20
6.1.2. Database regarding cases with a cross-border component	17	6.2.1.2. Germany	20
6.1.3. One-Stop-Shop Mechanism	17	6.2.1.3. Sweden	21
6.1.4. Mutual assistance	18	<b>6.3. DPA Survey – budget and staff</b>	<b>21</b>
6.1.5. Joint operations	19	6.3.1 Budget	21
<b>6.2. National cases</b>	<b>20</b>	6.3.2 Staffing	21

**7****TRANSPARENCY  
AND ACCESS TO  
DOCUMENTS** **22****8****STAKEHOLDER  
CONSULTATION** **23**

<b>8.1. Public consultations on draft guidance</b>	<b>23</b>
<b>8.2. Stakeholder survey on adopted guidance</b>	<b>23</b>
<b>8.3. Stakeholder events</b>	<b>24</b>

**9****MAIN OBJECTIVES  
FOR 2019** **25**

<b>9.1. Legal work plan</b>	<b>25</b>
9.1.1. Further guidance	25
9.1.2. Advisory role to the European Commission	26
9.1.3. Consistency measures	26
<b>9.2. Communications</b>	<b>26</b>

**10****CONTACT  
DETAILS** **27****11****ANNEXES** **28**

<b>11.1. General Guidance adopted in 2018</b>	<b>28</b>
<b>11.2. Expert Subgroups: scope of mandate</b>	<b>29</b>



# Foreword

2018 was a landmark year for data protection. On 25 May 2018, the long anticipated General Data Protection Regulation (GDPR) entered into application. In addition to updating the European Union's data protection rules for the digital age, this Regulation established the European Data Protection Board (EDPB) to ensure consistent application of the new rules across the EEA.

The EDPB is therefore a young EU body. Yet even in the first seven months of its existence, we have reached several milestones which we are now able to reflect upon.

Our role is to ensure the harmonised enforcement of the GDPR across the EEA. To this end, we endorsed the 16 GDPR related Guidelines of the Article 29 Working Party, we adopted 4 more Guidelines, 26 Opinions on Data Protection Impact Assessments carried out by the national Supervisory Authorities and held five plenary meetings addressing a range of topics, from the EU-Japan draft adequacy decision to electronic evidence and ePrivacy.

The feedback we have received from stakeholders on the first year of work has been encouraging. Many people and companies are now calling for increased global alignment

on the processing of personal data. We believe that by coordinating a consistent approach to data protection, the EU is demonstrating that respect for individuals' rights to privacy and data protection can go hand-in-hand with a flourishing economy, not least because it provides businesses with a clear framework and creates competitive advantages, such as improved customer loyalty and more efficient operations.

Next year is set to be even busier. At the beginning of 2019, we adopted our working programmes for 2019-2020. The EDPB work programme aims to address the priority needs of all stakeholders, including EU legislators. Having already issued guidance on the interpretation of new provisions introduced by the GDPR, the EDPB will now turn its attention to specific items and technologies.

In my view, with national Supervisory Authorities working together on an equal footing and the support of a dynamic Secretariat, the EDPB is well equipped for its mission of upholding a high level of data protection across the EEA. Looking ahead, I am confident that we will continue to lead by example in striving for transparency and cooperation in the EEA, and beyond.

**Andrea Jelinek**  
**Chair of the European Data Protection Board**

# 2



## Mission statement, tasks and principles

The European Data Protection Board (EDPB) aims to ensure the consistent application of the [General Data Protection Regulation](#) (GDPR) and of the [European Law Enforcement Directive](#) across the Economic European Area.

The EDPB can adopt general guidance to further clarify European data protection laws, giving stakeholders – including individuals – a consistent interpretation of their rights and obligations, and providing Supervisory Authorities with a benchmark for enforcing the GDPR.

The EDPB is also empowered to issue Opinions or Decisions (more precisely, ‘Consistency Opinions’ or ‘Consistency Decisions’) to guarantee a consistent application of the GDPR across the EEA by the national Supervisory Authorities.

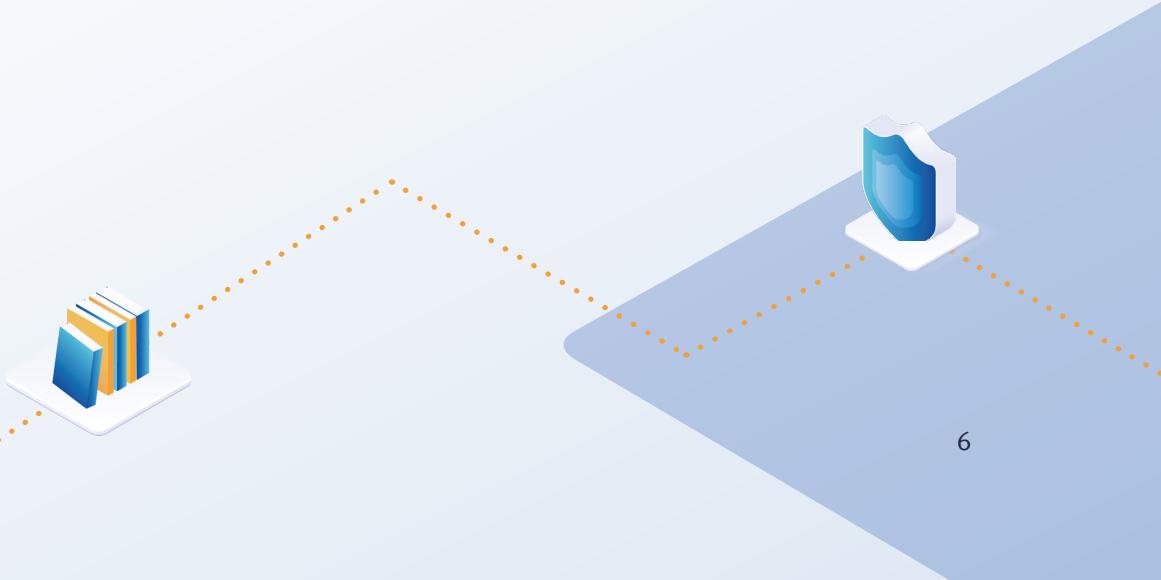
The EDPB acts in accordance with its [rules of procedure](#) and [guiding principles](#).

### 2.1. TASKS AND DUTIES

- The EDPB provides [general guidance](#) (including guidelines, recommendations and best practices) to clarify the law.
- The EDPB issues **Consistency** Opinions or Decisions to guarantee the consistent application of the GDPR.
- The EDPB promotes **cooperation** and the effective exchange of information and best practices between national Supervisory Authorities.
- The EDPB **advises** the European Commission on any issue related to the protection of personal data and new proposed legislation in the European Union.

## 2.2. GUIDING PRINCIPLES

- **Independence and impartiality.** The EDPB is an independent body, which performs its tasks and exercises its powers impartially.
- **Good governance,** integrity and good administrative behaviour. The EDPB acts in the public interest as an expert, trustworthy and authoritative body in the field of data protection, with good decision-making processes and sound financial management.
- **Collegiality and inclusiveness.** The EDPB is organised and acts collectively as a collegiate body, as established by the provisions of the GDPR and the Police and Criminal Justice Data Protection Directive.
- **Cooperation.** The EDPB promotes cooperation between Supervisory Authorities and endeavours to operate, where possible, by consensus, holding the GDPR and the Data Protection Directive as an overarching reference.
- **Transparency.** The EDPB carries out its work as openly as possible, so as to be more effective and more accountable to the public. The EDPB strives to explain its activities using clear language that is accessible to all.
- **Efficiency and modernisation.** The EDPB makes every effort to ensure that its work is as efficient and as flexible as possible, in order to achieve the highest level of cooperation between its members. The EDPB does this by using new technologies to keep working methods up to date, minimise formalities, and provide efficient administrative support.
- **Proactivity.** The EDPB undertakes its own initiatives, in order to anticipate and support innovative solutions that will help to overcome digital challenges to data protection. The EDPB encourages the effective participation of stakeholders (whether members, observers, staff or invited experts), so that their needs and aspirations can be fully taken into account.



# 3



## About the European Data Protection Board

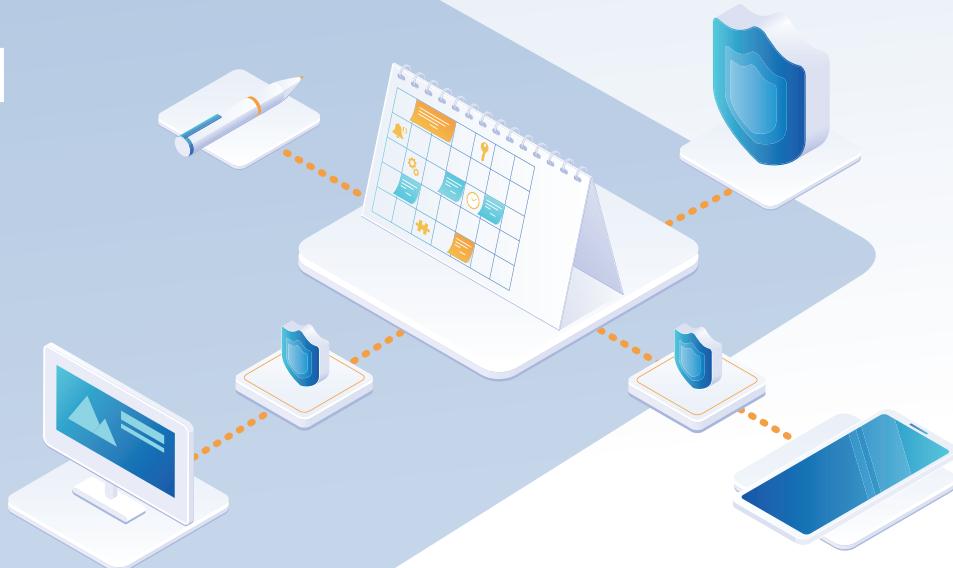
The European Data Protection Board is an independent European body, which contributes to the consistent application of data protection rules throughout the European Economic Area and promotes cooperation between the EEA's Data Protection Authorities.

The EDPB is composed of representatives of the national Data Protection Authorities and the European Data Protection Supervisor (EDPS). The Supervisory Authorities of the EEA EFTA States (Iceland, Liechtenstein and Norway) are also members with regard to GDPR-related matters, although they do not hold the right to vote nor can they be elected as chair or deputy chair.

The EDPB was established by the [General Data Protection Regulation \(GDPR\)](#). The European Commission and – with regard to GDPR-related matters – the European Free Trade Association (EFTA) Surveillance Authority have the right to participate in the activities and meetings of the Board, but without voting rights.

The EDPB has a [Secretariat](#), which is provided by the EDPS. A [Memorandum of Understanding](#) determines the terms of cooperation between the EDPB and the EDPS.

# 4



## 2018 – an overview

### 4.1. SETTING UP THE EDPB

#### 4.1.1 The Rules of Procedure

The [rules of procedure](#) were adopted during the first plenary meeting of the European Data Protection Board, which took place on 25 May 2018. These outline the most important operational rules of the Board. They describe:

- The EDPB's guiding principles
- The organisation of the EDPB
- The cooperation between its members
- The election of its chair and deputy chairs
- The EDPB's working methods

On 23 November 2018, the EDPB approved several changes to its rules of procedure. Among other things, the changes gave full effect to the European Economic Area (EEA) Joint Committee decision, integrating the General Data Protection Regulation

(GDPR) into the EEA agreement. The EEA EFTA Supervisory Authorities participate fully within the EDPB, without the right to vote or to be elected as chair or deputy chair.

#### 4.1.2 Organisation of Expert Subgroups

To assist in performing its tasks, several expert subgroups have been set up within the EDPB.

The establishment, suspension or termination of any expert subgroup may be decided upon at any time, following a proposal from the Chair or from at least three members of the Board. The list of expert subgroups is reviewed by the Board in the first plenary meeting of each year.

The list of the expert subgroups and their respective mandates are available under section 11.2.

## 4.2. SETTING UP THE SECRETARIAT

### 4.2.1. Memorandum of Understanding

The [Memorandum of Understanding](#) (MoU) determines the terms of cooperation between the European Data Protection Board and the European Data Protection Supervisor (EDPS). While the EDPS is a member of the EDPB, it also provides the Secretariat to the EDPB. The GDPR states that the Secretariat is required to perform all its tasks exclusively under the instructions of the Chair. These tasks involve providing analytical, administrative and logistical support to the EDPB.

The MoU establishes a clear separation between the functions assigned specifically to the EDPB Secretariat and the administrative support functions provided to the Secretariat by the EDPS, such as those related to human resources, working equipment, finance and budget. The EDPB Secretariat is in charge of the organisation of EDPB meetings and analytical support by drafting EDPB documents, as well as content-related duties, such as record management, the handling of access requests, local information security, public and press communications and the duties of the data protection officer.

In the interest of sound administration and consistent cooperation, the terms of the MoU were agreed upon by both the EDPB and the EDPS prior to the entry into force of the GDPR, during the first EDPB plenary meeting on 25 May 2018.

### 4.2.2. Preparation for 25 May 2018

To set up the EDPB Secretariat ahead of 25 May 2018, a dedicated EDPB Matters sector was created within the EDPS. Throughout 2017 and early 2018, this sector was responsible for carrying out the preparatory measures needed to create the EDPB. These included selecting and customising IT communication tools, preparing the EDPB's external communications, concluding agreements with other EU institutions for the externalisation of certain activities and developing legal agreements in cooperation with the national Supervisory Authorities (including the Memorandum of Understanding and the Rules of Procedure).

## 4.3. SETTING UP COOPERATION AND CONSISTENCY

### 4.3.1. IT Communications Tool (IMI)

Under the GDPR, the Supervisory Authorities (SAs) of EU Member States cooperate closely to ensure consistent protection of individuals' data protection rights across the European Union. One of their tasks is to assist one another and coordinate decision-making in cross-border data protection cases. Via the so-called consistency mechanism, the EDPB issues Consistency Opinions or Decisions. The EDPB binding Consistency Decisions aim to arbitrate in cases where national Data Protection Authorities take different positions in cross-border cases.

Via the so-called consistency mechanism, the EDPB issues Consistency Opinions or Decisions.

The Internal Market Information System (IMI) was chosen as the IT platform to support cooperation and consistency procedures under the GDPR. IMI helps public authorities cooperate and exchange information. The GDPR is the thirteenth legal area supported by the system.

IMI was developed by the European Commission's Directorate General for Internal Market, Industry, Entrepreneurship and SMEs (DG GROW). It has been adapted, in close cooperation with the EDPB Secretariat and in consultation with the national Supervisory Authorities, to suit the needs of the GDPR. Fourteen IMI modules, 19 forms and more than 10,000 data fields have been created to address the needs of Data Protection Authorities and the GDPR procedures.

On 25 May 2018, the first case was initiated in IMI and shortly afterwards Supervisory Authorities started to cooperate via the system. By the end of 2018, more than 255 cross-border cases were being examined.

# 5



## European Data Protection Board activities in 2018

The EDPB aims to ensure the consistent application of the [General Data Protection Regulation](#) (GDPR) and of the European [Law Enforcement Directive](#) across the European Union.

The EDPB can adopt general guidance to clarify European data protection laws. This provides stakeholders with a consistent interpretation of their rights and obligations and ensures that Supervisory Authorities have a benchmark for enforcing the GDPR.

The EDPB is also empowered to issue Opinions or Binding Decisions to guarantee the consistent application of the GDPR by the national Supervisory Authorities.

### 5.1. GENERAL GUIDANCE

During its first plenary meeting on 25 May 2018, the EDPB **endorsed 16 Guidelines** previously established by the Article 29 Working Party (WP29) (see Annex for full list).

During the remainder of 2018, the EDPB adopted four more Guidelines that aim to clarify a range of provisions under the GDPR. These Guidelines address certification and the identification of certification criteria, derogations relating to international transfers, the territorial scope of the GDPR and the accreditation of certification bodies.

### **5.1.1. Guidelines on Certification and identifying Certification Criteria**

During its first plenary meeting on 25 May 2018, the EDPB adopted a first version of the [Guidelines 01/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679](#).

The EDPB's guidance provides stakeholders with a consistent interpretation of their rights and obligations.

Achieving certification from an approved certification body is an element that may be used by organisations to demonstrate their compliance with EU data protection legislation.

As early as 2010, the Article 29 Working Party [established](#) that certification could play an important role in the accountability framework for data protection. The GDPR reinforced this principle, stating that the establishment of certification mechanisms can enhance transparency and compliance with the Regulation.

However, certification remains a voluntary process. The EDPB has therefore encouraged Member States and Supervisory Authorities (SAs) to establish certification mechanisms and provided guidance to clarify the role of SAs in this process.

Following the adoption of the first version of the document, a public consultation was launched and remained open for six weeks. A final version of the Guidelines was adopted in December 2018, taking into account the results of the consultation.

### **5.1.2. Guidelines on Derogations Applicable to international Transfers**

During its first plenary meeting, the EDPB adopted the [Guidelines 02/2018 on derogations of Article 49 under Regulation 2016/679 applicable to international transfers](#) that clarify how to interpret the derogations outlined under Article 49. The guidelines clarify the need to interpret those derogations in a restrictive manner, as they are exceptions to 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.

The Guidelines build on the work of the Article 29 Working Party, which conducted a public consultation on an initial version of the text. The EDPB took into consideration the input received and integrated the appropriate changes into the final version.

### **5.1.3. Guidelines on Territorial scope**

Article 3 of the GDPR determines the territorial scope of the Regulation and seeks, in the context of worldwide data flows, to establish a level playing field for companies operating in the EU. The territorial scope of the GDPR is based on two main criteria: the “establishment” criterion, outlined in Article 3(1), and the “targeting” criterion, outlined in Article 3(2).

The relevant provisions of the GDPR apply depending on which of these criteria are met. The “establishment” criterion refers to cases in which a controller or processor is established within the EU, regardless of whether the actual processing of personal data takes place in the EU or not. The “targeting” criterion applies to cases where a controller or processor is not established within the Union, but in which the processing of personal data involves offering goods or services to individuals in the EU or monitoring their behaviour.





During its fourth plenary meeting on 16 November 2018, the EDPB adopted a first version of the [Guidelines 03/2018 on the territorial scope of the GDPR](#), with the aim of providing a common interpretation for the application of these criteria. The Guidelines specify the various scenarios that may arise and how to address them. These include cases where the data controller or processor is established outside of the EU and cases in which the designation of a representative in the EU is required.

The Guidelines were subject to a public consultation.

#### 5.1.4. Guidelines on Accreditation

During its fifth plenary meeting on 4 December 2018, the EDPB adopted a revised version of the [Guidelines 04/2018 on the accreditation of certification bodies](#). The first version of the guidelines was adopted by the Article 29 Working Party and the revised version aimed to incorporate the feedback received during the public consultation. This issue of accreditation is addressed by Article 43 of the GDPR, which requires Member States to ensure that certification bodies responsible for issuing GDPR certifications are accredited by either or both the competent Supervisory Authority or the relevant national accreditation body. In cases where accreditation is carried out by the national accreditation body, the Article sets out the additional requirements that must also apply. The EDPB Guidelines aim to clarify the accreditation process.

A public consultation was held on the first version of the text by the Article 29 Working Party. The EDPB also adopted a new Annex providing guidance on the additional accreditation requirements to be established by the national Supervisory Authorities. This annex was subject to a new public consultation.

## 5.2. CONSISTENCY FINDINGS

### 5.2.1. Consistency Opinions

EEA national SAs must request an Opinion from the EDPB before adopting any decision on subjects specified by the GDPR having cross-border implications. This applies when a national SA:

- intends to adopt a list of the processing operations subject to the requirement for a data protection impact assessment (DPIA);
- intends to adopt a draft code of conduct relating to processing activities;
- aims to approve the criteria for accreditation of a certification body;
- aims to adopt standard data protection clauses or contractual clauses;
- aims to approve binding corporate rules.

The competent Supervisory Authority has to take utmost account of the opinion.

In addition, any Supervisory Authority, the Chair of the Board or the Commission may request that any matter of general application or which has consequences for more than one Member State be examined by the Board with a view to obtaining an Opinion. This can also apply in cases where a competent Supervisory Authority does not comply with obligations for mutual assistance or for joint operations.

The aim of these Opinions is to guarantee the consistent application of the GDPR by the national Supervisory Authorities.

Between 25 May and 31 December 2018, 26 Consistency Opinions on the national lists of processing operations subject to a DPIA were adopted by the EDPB. The purpose of the exercise was to ensure consistency across all national lists.

### 5.2.2. Binding Decisions

The EDPB can also act as a dispute resolution body. It adopts binding decisions to ensure the consistent application of the GDPR by the national Supervisory Authorities in the following cases:

- a dispute takes place within the One-Stop-Shop mechanism (a Concerned SA raises a relevant and reasoned objection which is not followed by the Lead SA);
- a disagreement occurs relating to which authority should take on the role of Lead SA;
- an SA does not request, or does not follow, a Consistency Opinion issued by the EDPB.

For more information on the operations of Lead SAs versus Concerned SAs, please see Chapter 6 of this report.

Between 25 May and 31 December 2018, no dispute resolutions were initiated. This suggests that, to date, SAs have been able to reach consensus on all current cross-border cases.

### 5.3. LEGISLATIVE CONSULTATION

The EDPB advises the European Commission on any issue related to the protection of personal data, on the format and procedures for information exchange between companies and SAs under Binding Corporate Rules (BCRs) and on certification requirements. The EDPB also advises the European Commission on the assessment of the adequacy of the level of data protection in third countries or international organisations.

In 2018, the EDPB issued two such Opinions: one on electronic evidence (e-Evidence) and one on the EU-Japan draft adequacy decision. The European Commission requested both of these Opinions.

As of 11 December 2018 - when the new data protection rules for the EU institutions came into force - the EDPB is also subject to Article 42 of [Regulation 2018/1725](#) on legislative consultation. This allows for the EDPS and the

EDPB to coordinate their work, with the intention of issuing a joint Opinion.

In 2018, the EDPB also adopted, on its own initiative, a statement on the draft ePrivacy Regulation.

#### 5.3.1. e-Evidence

During its Third Plenary Session, which took place on 25 and 26 September 2018, the EDPB adopted the Opinion 23/2018 on the Regulation on [European Production and Preservation Orders for electronic evidence in criminal matters](#), proposed by the European Commission in April 2018.

The EDPB stressed that the proposed new rules providing for the collection of electronic evidence should sufficiently safeguard individuals' data protection rights whilst aligning more closely with EU data protection law.

#### 5.3.2. EU-Japan draft adequacy decision

During the Fifth Plenary Session of the EDPB, which took place on 4-5 December 2018, the EDPB Members adopted the Opinion 28/2018 regarding the [European Commission Draft Implementing Decision on the adequate protection of personal data in Japan](#), which the EDPB received in September 2018.

The EDPB's key objective was to assess whether the European Commission had ensured that the Japanese framework provided for an adequate level of data protection for individuals, essentially equivalent to the standard set out in the GDPR. The EDPB made its assessment based on the documentation provided by the Commission.

The GDPR requires that, in order to be considered adequate, any non-EU country's legislation must be aligned to the principles and concepts enshrined in the GDPR, as well as to general aspects of EU law, including the rule of law.

There were key areas of alignment between the GDPR framework and the Japanese framework on certain core

provisions. In addition, the EDPB welcomed the efforts made by the European Commission and the Japanese Personal Information Protection Commission (PPC) to increase this convergence.

However, the EDPB noted that a number of concerns remained, particularly relating to the notion of consent, which includes the right to withdraw consent, to transparency obligations and to access to the redress system. The EDPB also requested further clarification on the role of the data processor and on the extent of the restrictions to the rights of individuals set out in Japanese legislation, as well as assurance that personal data transferred from the EU to Japan would be closely monitored during the whole “life cycle” of the transfer.

Some of those elements were taken into account in the revised adequacy decision adopted by the European Commission on 23 January 2019.

### **5.3.3. Statement on ePrivacy**

During its first plenary meeting of 25 May 2018, the EDPB adopted a [statement](#) on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications.

This statement includes a call for a swift adoption of the new ePrivacy Regulation and some suggestions on some specific issues relating to proposed amendments by the co-legislators.

## **5.4. OTHER DOCUMENTS**

### **5.4.1. Letter to ICANN**

During the Second Plenary Session of the EDPB, on 4 and 5 July 2018, the EDPB adopted a [letter](#) addressed to Mr Göran Marby, President and CEO of the Board of Directors of the Internet Corporation for Assigned Names and Numbers

(ICANN). The letter provided guidance to help ICANN to develop a GDPR-compliant model for access to personal data processed in the context of WHOIS. The WHOIS system provides a register for domain names and IP addresses.

The letter addressed the issues of purpose specification, collection of “full WHOIS data”, registration of legal persons, logging of access to non-public WHOIS data, data retention and codes of conduct and accreditation.

The EDPB expects ICANN to develop and implement a WHOIS model that will enable the legitimate use of personal data concerning those registered in the WHOIS system, specifically by relevant stakeholders such as law enforcement, without leading to an unlimited publication of such data.

### **5.4.2. Letter on the PSD2 Directive**

The EDPB adopted a second [letter](#) in July 2018. Addressed to Sophie in't Veld, Member of the European Parliament, it aimed to respond to her request for further clarification on a number of issues relating to the revised Payments Services Directive (PSD2 Directive) and the protection of personal data. The PSD2 Directive concerns payment services in the EU's internal market. In this letter, the EDPB aimed to clarify:

- the concept of “silent party data” and the processing of this data by Third Party Providers;
- procedures for giving and withdrawing consent;
- Regulatory Technical Standards;
- cooperation between banks and the European Commission, the EDPS and the WP29;
- any other data protection gaps remaining.

The EDPB also expressed its wish for a dialogue between competent EU bodies (particularly data protection and financial Supervisory Authorities) in order to set up a coordinated approach aimed at ensuring strengthened and consistent protection for EU citizens.

#### 5.4.3. Statement on Economic Concentration

In August 2018, the EDPB adopted a [statement](#) on the impact of economic concentration on data protection via written procedure. The statement followed the European Commission's announcement that it intended to analyse the effects of further concentration of 'commercially sensitive data about customers' personal data in the context of its investigation into the proposed acquisition of Shazam by Apple. The EDPB considered it essential to assess longer-term implications for the protection of economic, data protection and consumer rights whenever a significant merger is proposed, particularly in technology sectors of the economy. The Board went on to note that increased market concentration in digital markets has the potential to threaten the level of data protection and freedom enjoyed by consumers of digital services. The data protection and privacy interests of individuals are relevant to any assessment of potential abuse of dominance as well as mergers of companies, which may accumulate or which have accumulated significant informational power. The statement concluded that independent Data Protection Authorities can help with the assessment of such an impact on the consumer or society more generally in terms of privacy, freedom of expression and choice.

#### 5.5. PLENARY MEETINGS AND EXPERT SUBGROUPS

Between 25 May and 31 December 2018, the EDPB held five plenary sessions. During these sessions the EDPB Members adopted guidance and requests for mandates for the relevant expert subgroups and practical matters related to the functioning of the Secretariat.

In addition, there were 36 expert subgroup meetings. The different expert subgroups focus on specific areas of data protection and assist the EDPB in performing its tasks.

The list of the expert subgroups and their respective mandates are available below in section 11.2.

The EDPB expressed its wish for a dialogue between competent EU bodies aimed at ensuring strengthened protection for EU citizens.

# 6



## Supervisory Authority activities in 2018

Under the GDPR, the Supervisory Authorities have a duty to cooperate in order to ensure consistent application of the Regulation. In cases with a cross-border component, the Supervisory Authorities of the European Economic Area (the 28 EU Member States plus Iceland, Norway and Liechtenstein) have a range of tools at their disposal to facilitate harmonisation. These are:

- mutual assistance;
- joint operation;
- the One-Stop-Shop cooperation mechanism.

### 6.1. CROSS-BORDER COOPERATION

#### 6.1.1. Preliminary Procedure to Identify the Lead and Concerned Supervisory Authorities

Before starting a One-Stop-Shop procedure for a cross-border case, it is necessary to identify the authority that will lead the investigation (Lead SA) and the other Concerned Supervisory Authorities (Concerned SA or SAs). The Lead SA will lead the investigation and draft the decision, while the Concerned SAs will have the opportunity to raise objections.

The Lead SA is the authority within the EEA where the controller or processor under investigation has its main establishment. For example, the place of central administration is one of the criteria used to identify the main establishment of a controller or processor.

## The Lead SA is the authority within the EEA where the controller or processor under investigation has its main establishment.

Further information on this subject is available in Article 1.2 of the [Article 29 Working Party Guidelines on identifying a controller or processor's lead Supervisory Authority](#).

The EDPB created workflows in the Internal Market Information (IMI) system to enable the SAs to identify their respective roles. This IT platform is used to support cooperation and consistency procedures under the GDPR. The main purpose of this procedure is to define their roles at an early stage and to avoid objections relating to competencies later on.

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

In 2018, 574 procedures were initiated to identify the Lead SA and the Concerned SAs in cross-border cases. Of these 574 procedures, 274 have been closed.

In 2018, no dispute on the selection of the Lead SA occurred.

### **6.1.2. Database Regarding Cases with a Cross-Border Component**

A cross-border case emerges where the controller or the processor has an establishment in more than one Member State, or where the data processing activity substantially affects individuals in more than one Member State.

Cases with a cross-border component are registered in a central database from which the aforementioned procedures can be initiated.

Between 25 May and 31 December 2018, 255 cases with a cross-border component were registered in the IMI system. Most of the cases derived from complaints by individuals (176 cases). The rest (79 cases) originated from other sources, such as an investigation, an SA initiative, a legal obligation or a media report.

The three main topics of these cases related to data subjects' rights, consumer rights, and data breaches.

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

### **6.1.3. One-Stop-Shop Mechanism**

The GDPR establishes a specific cooperation procedure (One-Stop-Shop) for cross-border cases.

The One-Stop-Shop mechanism demands cooperation between the Lead SA and the Concerned SA. The Lead SA leads the investigation and plays a key role in the process of reaching consensus between the Concerned SAs, in addition to working to reach a coordinated decision with regard to the data controller or processor.



The Lead SA must first investigate the case while observing national procedural rules, ensuring that the affected individuals are able to exercise their right to be heard, for example. During this investigation phase, the Lead SA can gather information from another Supervisory Authority via mutual assistance or by conducting a joint investigation.

## If a dispute arises on the draft decision and no consensus can be found, the consistency mechanism is triggered and the case is referred to the EDPB.

The IMI system also gives the Lead SA the opportunity to launch informal communication with all Concerned SAs, in order to collect information.

Once the Lead SA has completed its investigation, it prepares a draft decision and communicates it to the Concerned SAs. They have the right to object. This either leads to a revised draft decision or, if no consensus can be found, triggers the EDPB's dispute resolution mechanism.

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

If the Concerned SAs do not object to the initial draft decision, or to the revised one, they are deemed in agreement with the draft decision.

The IMI system offers different procedures to follow when handling One-Stop-Shop cases:

- informal consultation procedures;
- draft decisions or revised decisions submitted by the Lead SA to the Concerned SAs;
- final One-Stop-Shop decisions submitted to the Concerned SAs and to the EDPB.

Between 25 May and 31 December 2018, 43 One-Stop-Shop procedures were initiated by SAs from 14 different EEA countries. At the end of the year, the procedures were at different stages: 20 were at the informal consultation level, 20 were at draft decision level and two were final decisions.

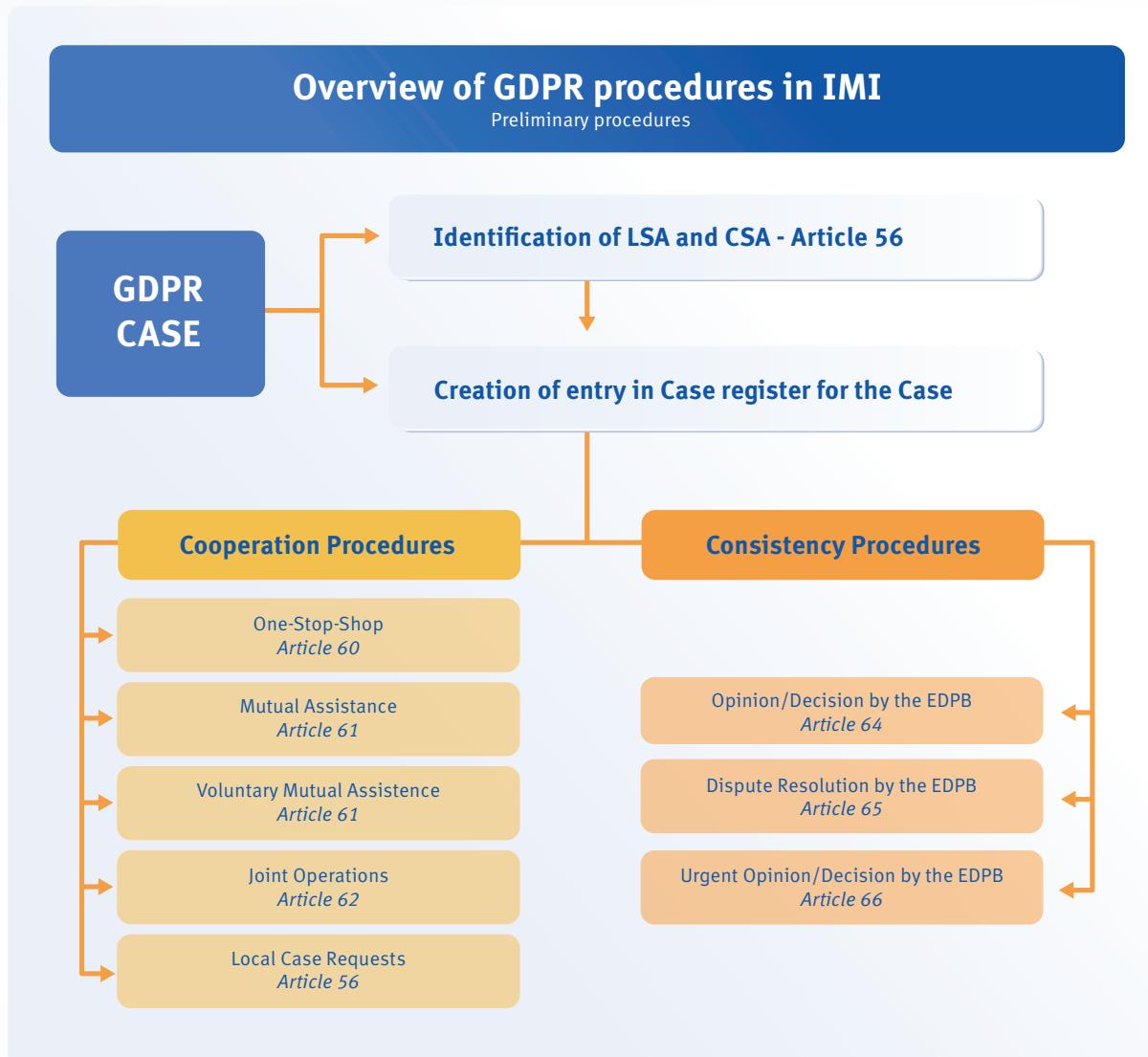
These first One-Stop-Shop final decisions related to the exercise of the rights of individuals (such as the right to erasure), the appropriate legal basis for data processing and data breach notifications.

The limited number of One-Stop-Shop procedures to date can be explained by the fact that the draft decisions produced by Lead SAs result from the investigations they have conducted with respect to the relevant national administrative procedural laws. However, an increase has been observed in the number of One-Stop-Shop procedures being launched.

### **6.1.4. Mutual assistance**

The mutual assistance procedure allows for Supervisory Authorities to ask for information from other SAs, but also to request other measures for effective cooperation, such as prior authorisations or investigations.

Mutual assistance can be used for cross-border cases subject to the One-Stop-Shop procedure, either as part of the preliminary phase, to gather the necessary information before drafting a decision, or for national cases with a cross-border component.



The IMI system enables the use of either informal mutual assistance without any legal deadline or the use of formal mutual assistance, whereby the SA from which information has been requested has a legal deadline of one month to reply.

In the period between 25 May and 31 December 2018, 397 mutual assistance requests, both formal and informal, were triggered. 89% of the requests were replied to within 23 days.

#### 6.1.5. Joint operations

The GDPR allows for Supervisory Authorities to carry out joint investigations and joint enforcement measures. Similarly to the mutual assistance procedure, joint operations can be used in the context of cross-border cases subject to the One-Stop-Shop procedure or for national cases with a cross-border component.



## 6.2. NATIONAL CASES

In 2018, the Supervisory Authorities of the 31 EEA countries reported over a hundred thousand cases at national level. The majority of cases were either related to complaints or were initiated on the basis of data breach notifications from controllers.

Supervisory Authorities have different corrective measures at their disposal. These are:

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

### 6.2.1. Some relevant national cases with exercise of corrective powers<sup>1</sup>

#### 6.2.1.1. Austria

On 12 September 2018, the Austrian Data Protection Authority (DPA) took its first administrative penal decision relating to infringements of the GDPR and the Austrian Data Protection Act.

The Austrian DPA imposed a fine on a Limited Liability Company running a sports betting café. This company was defined, within the meaning of Article 4(7) of the GDPR, as the controller of an image processing system, specifically, video surveillance. The cameras in question had been in use at least since 22 March 2018.

The Austrian DPA found that the controller violated several articles of the GDPR as well as provisions of the Austrian Data Protection Act (DSG), since public areas were involved in the surveillance but the company failed to delete any of the personal image data recorded. The Limited Liability Company was therefore issued with administrative fines amounting to 5,280 EUR.

The controller lodged a complaint with the Federal Administration Court appealing this decision.

#### 6.2.1.2. Germany

On 21 November 2018, the Supervisory Authority of **Baden-Württemberg** imposed the first German fine under the GDPR. Due to a violation of Article 32 of the GDPR on the Security of Processing, a German social network operator was fined 20,000 EUR.

The company had notified the Supervisory Authority of a data breach occurring in July 2018, in accordance with Article 33 of the GDPR. In their notification, they reported that the personal data of 330,000 users, such as e-mail addresses and passwords, had been hacked. The company cooperated fully and provided information on internal structures, which showed that passwords had been stored unencrypted. The company thereby failed to ensure data security according to Article 32(a) of the GDPR.

Due to its exemplary cooperation and readiness to follow all of the SA's recommendations, and taking into account the financial burden of the implementation costs and the initial fine, the company was not issued with any further fines.

At the federal level, the **German Supervisory Authority** imposed a fine of 1,500 EUR in application of the GDPR. The fine was issued in December 2018 due to a failure to cooperate with the Authority.

Other fines issued under the GDPR in Germany in 2018 included:

- two fines issued by the federal state of **Mecklenburg-Western Pomerania**, totalling 1,500 EUR;
- thirty-six fines issued by the Data Protection Authority of **North Rhine-Westphalia**, under Article 83(5) of the GDPR, amounting to 15,600 EUR;
- six fines issued by the DPA of the federal state of **Saarland**. These included one fine issued under Article 58(1) of the GDPR, two issued under Article 58(2) and three issued under Article 83(5).

#### 6.2.1.3. Sweden

At the end of May 2018, the Swedish Data Protection Authority initiated an audit of several organisations to see whether data protection officers had been appointed in accordance with the GDPR. After examining more than 350 companies and authorities, the audit results were published in October 2018.

The audit showed that the majority of the authorities and companies investigated had notified and appointed a data protection officer on time. However, the Swedish DPA identified deficiencies in approximately 16% of cases. There was only a marginal difference in compliance between public authorities and private sector companies.

Out of 66 scrutinised cases, the Swedish DPA issued 57 reprimands. In two other cases, the DPA issued the audited organisation with an order to comply, while seven cases were closed without further measures taken.

### 6.3. DPA SURVEY – BUDGET AND STAFF

Under the new legal framework, SAs have received new harmonised tasks and powers. They wield greater enforcement and investigation powers, they handle individuals' complaints, have to promote awareness on data protection law and are also required to cooperate with the other Supervisory Authorities. This implies a need for increased budgets and more staff members.

#### 6.3.1 Budget

Based on information provided by SAs from 26 EEA countries and the EDPS, an increase in the budget for 2018 and 2019 has in most cases occurred. However, the budget of two SAs decreased, while in three cases there were no changes. According to information provided by the respective SAs, the lack of changes can be explained by the application of biannual plans spanning this period.

**Under the new legal framework, SAs have received new harmonised tasks and powers. This implies a need for increased budgets and more staff members.**

Most of the SAs (17) stated that they required a budget increase of around 30-50% to perform their duties. However, almost none of the SAs received the requested amount. In some extreme cases, SAs have a need for up to double their current budget.

#### 6.3.2 Staffing

Based on information provided by SAs from 26 EEA countries and the EDPS, a majority of SAs have increased their staff numbers. However, in eight SAs the number of employees did not increase, while in one SA there was a decrease in staff numbers. Differences in personnel requirements across SAs is to be expected, given the varied remits of the SAs.

# 7



## Transparency and access to documents

Transparency is a core principle of the EDPB. As an EU institution, the EDPB is subject to [Article 15 of the TFEU](#) and [Regulation 1049/2001](#) on public access to documents. Article 76(2) of the GDPR and Article 32 of the EDPB's Rules of Procedure reinforce this requirement.

Upholding the principle of transparency means that any citizen of the European Union and any natural or legal person residing or having its registered office in a Member State has a right of access to EDPB documents. This right applies to all documents held by the EDPB, concerning any matter relating to its responsibilities.

In exceptional cases, the EDPB can refuse to disclose a document, or part of it. The reasons for refusal and other procedural rules are outlined in the [EU Public Access Regulation](#).

In 2018, the number of public access requests received for documents held by the EDPB was ten.

To ensure transparency, the EDPB also publishes the agendas and plenary sessions attended by the EDPB on its website. In 2019, the EDPB will continue to implement measures designed to increase the transparency of its work.

All citizens who believe they have been unjustifiably refused access can lodge a complaint with the European Ombudsman, or bring an action before the Court of Justice of the European Union.

# 8



## Stakeholder consultation

### 8.1. PUBLIC CONSULTATIONS ON DRAFT GUIDANCE

The EDPB organises public consultations to gather the views and concerns of all interested stakeholders and citizens. In 2018, the EDPB issued three consultations on its draft Guidelines:

- In May, the EDPB opened a public consultation on the [Guidelines on certification \(1/2018\)](#);
- In November, the EDPB opened a public consultation on the [Guidelines on the territorial scope of the GDPR \(3/2018\)](#);
- In December, the EDPB opened a public consultation on the [Annex 1 of the Guidelines on the accreditation of certification bodies \(4/2018\)](#).

### 8.2. STAKEHOLDER SURVEY ON ADOPTED GUIDANCE

A survey was conducted on adopted guidance as part of the annual review of European Data Protection Board activities under Article 71 of the General Data Protection Regulation. It focused on 20 GDPR Guidelines with questions concerning both their content and the adoption process, with a view to establishing stakeholders' opinions on their quality and usefulness.

In order to increase the reach of the questionnaire and the diversity of those responding to it, the EDPB invited 114 pan-European organisations to participate in the survey. They represent different geographies, sectors and business sizes.



Fifty-three responses were submitted. The results showed that participants had consulted, on average, eight Guidelines. The majority of the contributors were based in Europe (41 entities) as opposed to ten headquartered in North America and two in the Asia-Pacific region.

## The outcome of the survey confirms that Guidelines are seen as useful and pragmatic.

Sixty-five percent of stakeholders considered the Guidelines to be useful. While 45 percent considered them to be sufficiently pragmatic and operational for their needs, 23 percent called for improvement. For instance, they recommended shorter and more pragmatic guidance, not stricter than the GDPR, and to avoid contradictions between EDPB and national guidance. While half of the respondents judged the Guidelines to provide sufficient examples in their respective area of regulation, 16 percent called for the inclusion of more sophisticated case studies. Smaller businesses, with less expertise in data protection, favoured easier texts. The Guidelines were also judged positively as regards accessibility. Sixty-one percent of those who responded to the survey found the Guidelines easy to read, while 64 percent considered them easily accessible on the EDPB's website.

Most feedback concerning the consulting and drafting process of the Guidelines was positive or neutral. Some stakeholders encouraged the EDPB to increase opportunities to be involved and cooperate in the drafting of Guidelines.

The outcome of the survey confirms that, while the Guidelines are generally seen as useful, there is an understandable difference in their application depending on the sector, size and level of expertise of the stakeholder. The feedback was highly valued by the EDPB, as it moves to adopt further guidance in the next two years aimed at clarifying the GDPR provisions.

### 8.3. STAKEHOLDER EVENTS

The EDPB values the transparency of its activities. Its work programme, therefore, establishes the EDPB's commitment to creating increased opportunities for stakeholder engagement, such as the launch of stakeholder events.

During its last plenary meeting of 2018, the EDPB decided to organise two stakeholder events to collect views before adopting Guidelines on specific topics. The respective topics were the update of the 2010 Opinion of the Article 29 Working Party on the concepts of Controller and Processor and the elaboration of EDPB Guidelines on the Payment Services Directive (PSD2). The events were scheduled to take place in 2019.



# 9



## Main objectives for 2019

Having turned one on 25 May 2019, the EDPB is now looking ahead, evaluating where its focus should be in 2019 and beyond.

### 9.1. **LEGAL WORK PLAN**

At the beginning of 2019, the EDPB adopted a two-year work programme for 2019-2020. This is based on the priority needs of all stakeholders, including the EU legislator, as identified by EDPB members. Three areas of interest were identified for the coming two years, as outlined below.

The EDPB adopted a two-year work programme for 2019-2020.

#### 9.1.1. **Further Guidance**

The EDPB will adopt further Guidelines to ensure consistent interpretation of the GDPR across the EU, enabling stakeholders and Supervisory Authorities to apply the provisions of the GDPR in a harmonised manner.

In 2019 and 2020, the EDPB aims to focus on data subjects' rights, the concept of the controller and processor and legitimate interest. The EDPB will also consider technologies such as connected vehicles, blockchain, artificial intelligence and digital assistants, video surveillance, search engine delisting and data protection by design and by default.

### 9.1.2. Advisory Role to the European Commission

The EDPB will continue to advise the Commission on issues such as cross-border data access requests for e-Evidence, the revision or introduction of adequacy decisions for data transfers to third countries and any possible revision of the EU-Canada Passenger Name Record (PNR) agreement.

### 9.1.3. Consistency Measures

In cross-border cases where consensus cannot be found between the Lead SAs and Concerned SAs within the relevant cooperation procedure, the EDPB will act as a dispute resolution body and issue binding decisions.

In addition, the EDPB will continue to deliver Consistency Opinions to Supervisory Authorities in line with Article 64 of the GDPR. These include cases such as the SAs' draft approval of cross-border codes of conduct, certification criteria and binding corporate rules to ensure the transfer of data within multinationals.

## 9.2. COMMUNICATIONS

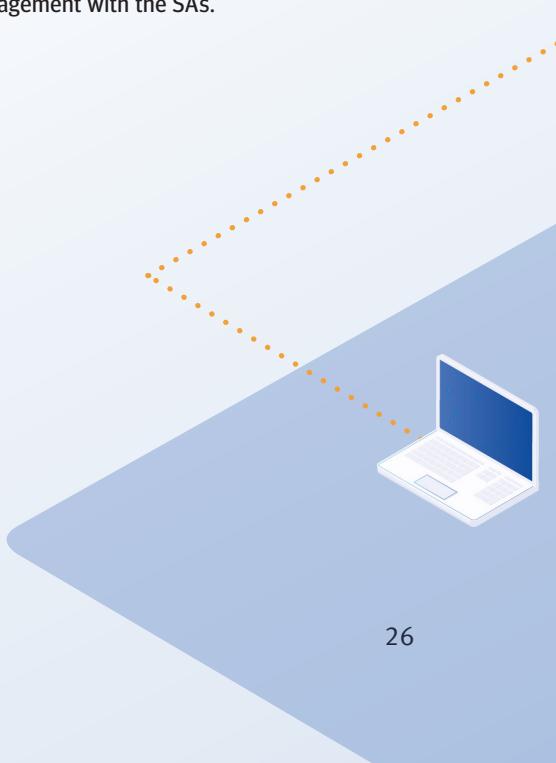
The EDPB ensures full transparency of its work among media, the public and stakeholders from across the public and private sectors. This is particularly vital at a time when there is a heightened public focus on data protection and privacy issues.

In 2019, the EDPB will continue this mission by deepening existing stakeholder relationships and developing new ones with relevant parties.

The EDPB Members are fully committed to continuing their participation in relevant conferences and speaking engagements, as well as maintaining a strong social media presence to drive public engagement with the EDPB's activities.

The EDPB will continue its mission by deepening existing stakeholder relationships and developing new ones with relevant parties.

Given that a significant part of the EDPB's work relies on its cooperation with the Supervisory Authorities, the EDPB is keen to support a harmonised communication approach. This will be further developed in 2019, via the network of Data Protection Authorities press and communications officers, as well as through supporting the EDPB Chair in her outreach and engagement with the SAs.



# 10

## Contact details

**Postal address:**

Rue Wiertz 60, B-1047 Brussels

**Office address:**

Rue Montoyer 30, B-1000 Brussels

**Email:**

[edpb@edpb.europa.eu](mailto:edpb@edpb.europa.eu)

# 11

## Annexes

### 11.1. GENERAL GUIDANCE ADOPTED IN 2018

1. [Guidelines on consent under Regulation 2016/679, WP259 rev.01](#)
2. [Guidelines on transparency under Regulation 2016/679, WP260 rev.01](#)
3. [Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01](#)
4. [Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01](#)
5. [Guidelines on the right to data portability under Regulation 2016/679, WP242 rev.01](#)
6. [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](#)
7. [Guidelines on Data Protection Officers \('DPO'\), WP243 rev.01](#)
8. [Guidelines for identifying a controller or processor's lead supervisory authority, WP244 rev.01](#)
9. [Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30\(5\) GDPR](#)
10. [Working Document Setting Forth a Co-Operation Procedure for the approval of “Binding Corporate Rules” for controllers and processors under the GDPR, WP 263 rev.01](#)
11. [Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, WP 264](#)
12. [Recommendation on the Standard Application form for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, WP 265](#)
13. [Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, WP 256 rev.01](#)
14. [Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, WP 257 rev.01](#)
15. [Working Document on Adequacy Referential, WP 254 rev.01](#)
16. [Guidelines on the application and setting of administrative fines for the purpose of the Regulation 2016/679, WP 253](#)
17. [EDPB Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679](#)
18. [EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679](#)
19. [EDPB Guidelines 3/2018 on the territorial scope of the GDPR \(Article 3\) - version for public consultation](#)
20. [EDPB Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation \(2016/679\)](#)

## 11.2. EXPERT SUBGROUPS: SCOPE OF MANDATE

NAME OF SUBGROUP	SCOPE OF MANDATE
<b>Borders, Travel &amp; Law Enforcement (BTLE) Expert Subgroup</b>	<ul style="list-style-type: none"> <li>• Law enforcement directive</li> <li>• Cross-border requests for e-evidence</li> <li>• Adequacy Decisions, access to transferred data by law enforcement and national intelligence authorities in third countries (e.g. Privacy Shield)</li> <li>• Passenger Name Records (PNR)</li> <li>• Border controls</li> <li>• Preparation of the coordinated supervision under Art. 62 1725/2018</li> </ul>
<b>Compliance, e-Government and Health Expert Subgroup</b>	<ul style="list-style-type: none"> <li>• Code of conduct, certification and accreditation</li> <li>• Close cooperation on DPIA with the Technology ESG focusing on the perspective of their mandates</li> <li>• Close cooperation on privacy by design and by default with the Technology ESG focusing on the perspective of their mandates</li> <li>• Compliance with public law and eGovernment</li> <li>• Health</li> </ul>
<b>Cooperation Expert Subgroup</b>	<ul style="list-style-type: none"> <li>• General focus on procedures of the GDPR</li> <li>• Guidance on procedural questions</li> <li>• International mutual assistance and other cooperation tools to enforce the GDPR outside the EU (Art. 50)</li> </ul>
<b>Coordinators Expert Subgroup</b>	<ul style="list-style-type: none"> <li>• General coordination between the Expert Subgroup Coordinators</li> <li>• Coordination on the annual Expert Subgroup working plan</li> </ul>

NAME OF SUBGROUP	SCOPE OF MANDATE
<b>Enforcement Expert Subgroup</b>	<ul style="list-style-type: none"> <li>• Including exchange of information on concrete cases</li> <li>• Mapping/analysing the need for additional clarifications or guidance, based on practical experiences with the application of Chapters VI, VII and VIII of the GDPR, including mapping/analysing possible updates of existing Cooperation subgroup tools)</li> <li>• Monitoring of investigation activities</li> <li>• Practical questions on investigations</li> <li>• Guidance on the application of Chapter VIII of the GDPR together with the Fining TF</li> </ul>
<b>Financial Matters Expert Subgroup</b>	<p>Application of data protection principles in the financial sector, more specifically:</p> <ul style="list-style-type: none"> <li>• Automatic exchange of personal data for tax purposes</li> <li>• FATCA</li> <li>• Administrative arrangements for the transfer of personal data between EEA Financial Supervisory Authorities and non-EEA Financial Supervisory Authorities for cooperation purposes (ESMA)</li> </ul> <p>Interplay between Second Payment Services Directive (PSD2) and GDPR</p>
<b>International Transfers Expert Subgroup</b>	<p>Guidance on Chapter V: International transfer tools and policy issues, more specifically:</p> <ul style="list-style-type: none"> <li>• Review European Commission Adequacy decisions</li> <li>• Guidelines on Art. 46 of the GDPR and review of administrative arrangements between public authorities and bodies (e.g. ESMA)</li> <li>• Codes of conduct and certification as transfer tools</li> <li>• Art. 48 of the GDPR together with BTLE ESG</li> <li>• Art. 50 of the GDPR together with Cooperation ESG</li> <li>• Guidelines on territorial scope and the interplay with Chapter V of the GDPR - interaction with Key Provisions ESG</li> <li>• Exchange of information on review of BCRs and ad hoc contractual clauses according to Art. 64 of the GDPR</li> </ul>

NAME OF SUBGROUP	SCOPE OF MANDATE
<b>IT Users Expert Subgroup</b>	Developing and testing IT tools used by the EDPB with a practical focus: collecting feedback on the IT system from users, adapting the systems and manuals as well as discussing other business needs including tele- and videoconference systems
<b>Key Provisions Expert Subgroup</b>	Guidance on Chapters I (e.g. scope, definitions like LSA and large scale processing) and II (main principles) and on core concepts and principles of the GDPR, including Chapters III (e.g. rights of individuals, transparency), IV (e.g. DPO – shared competences with Compliance Tools ESG, Enforcement ESG and Technology ESG) and IX
<b>Social Media Expert Subgroup</b>	<ul style="list-style-type: none"> <li>• Analyzing social media services, conceived as online platforms that focus on enabling the development of networks and communities of users, among which information and content is shared and whereby additional functions provided by social media services include targeting, personalisation, application integration, social plug-ins, user authentication, analytics and publishing</li> <li>• Analysing established and emerging functions offered by social media, including the underlying processing activities and corresponding risks for the rights and freedoms of individuals</li> <li>• Developing guidance, recommendations and best practices in relation to both the offer and use of social media functions, in particular for economic or political reasons.</li> <li>• Providing assistance to other subgroups, in particular by proposing strategic priorities in terms of (a) supervision and (b) the development of new EDPB guidance or updating of existing WP29 guidance</li> </ul>

NAME OF SUBGROUP	SCOPE OF MANDATE
<b>Strategic Advisory Expert Subgroup</b>	<ul style="list-style-type: none"><li>• Guidance on strategic questions affecting the whole EDPB (including the discussion on the work plans of the ESGs)</li><li>• Clarification of questions that could not be resolved in the ESG</li></ul>
<b>Taskforce on Administrative Fines</b>	Development of guidelines on the harmonisation of the calculation of fines
<b>Technology Expert Subgroup</b>	<ul style="list-style-type: none"><li>• Technology, innovation, information security, confidentiality of communication in general</li><li>• ePrivacy, encryption</li><li>• DPIA and data breach notifications</li><li>• Emerging technologies, innovation and other challenges related to privacy: reflecting on data protection risks of future technological developments</li><li>• Providing input on technology matters relevant to other ESGs</li></ul>



@eu\_edpb



eu-edpb



edpb.europa.eu



European Data Protection Board

# 2018

ANNUAL REPORT - EXECUTIVE SUMMARY

## COOPERATION & TRANSPARENCY



# TABLE OF CONTENTS

<b>1</b>	
FOREWORD	2
<b>2</b>	
ABOUT THE EUROPEAN DATA PROTECTION BOARD	3
<b>3</b>	
2018 SETTING UP OF THE EDPB AND THE SECRETARIAT – AN OVERVIEW	5
3.1. EDPB's activities	5
3.2. Supervisory Authorities' activities	6
3.3. Consultations	6
<b>4</b>	
MAIN OBJECTIVES FOR 2019	7



2018 was a landmark year for data protection. On 25 May 2018, the long anticipated General Data Protection Regulation (GDPR) entered into application. In addition to updating the European Union's data protection rules for the digital age, this Regulation established the European Data Protection Board (EDPB) to ensure consistent application of the new rules across the EEA.

The EDPB is therefore a young EU body. Yet even in the first seven months of its existence, we have reached several milestones which we are now able to reflect upon.

Our role is to ensure the harmonised enforcement of the GDPR across the EEA. To this end, we endorsed the 16 GDPR related Guidelines of the Article 29 Working Party, we adopted four more Guidelines, 26 Opinions on Data Protection Impact Assessments carried out by the national Supervisory Authorities and held five plenary meetings addressing a range of topics, from the EU-Japan draft adequacy decision to electronic evidence and ePrivacy.

The feedback we have received from stakeholders on the first year of work has been encouraging. Many people and companies are now calling for increased global alignment

on the processing of personal data. We believe that by coordinating a consistent approach to data protection, the EU is demonstrating that respect for individuals' rights to privacy and data protection can go hand-in-hand with a flourishing economy, not least because it provides businesses with a clear framework and creates competitive advantages, such as improved customer loyalty and more efficient operations.

Next year is set to be even busier. At the beginning of 2019, we adopted our working programmes for 2019-2020. The EDPB work programme aims to address the priority needs of all stakeholders, including EU legislators. Having already issued guidance on the interpretation of new provisions introduced by the GDPR, the EDPB will now turn its attention to specific items and technologies.

In my view, with national Supervisory Authorities working together on an equal footing and the support of a dynamic Secretariat, the EDPB is well equipped for its mission of upholding a high level of data protection across the EEA. Looking ahead, I am confident that we will continue to lead by example in striving for transparency and cooperation in the EEA, and beyond.

**Andrea Jelinek**  
Chair of the European Data Protection Board



# 2



## About the European Data Protection Board

The European Data Protection Board is an independent European body, established by the [General Data Protection Regulation \(GDPR\)](#), which contributes to the consistent application of data protection rules throughout the European Economic Area (EEA) and promotes cooperation between its data protection authorities.

The EDPB aims to ensure the consistent application in the European Economic Area of the GDPR and of the European [Law Enforcement Directive](#).

The EDPB can adopt general guidance to further clarify European data protection laws, giving stakeholders – including individuals – a consistent interpretation of their rights and obligations and providing supervisory authorities with a benchmark for enforcing the GDPR.

The EDPB is also empowered to issue opinions or decisions

to guarantee the consistent application of the GDPR by the national Supervisory Authorities ('Consistency Opinions' or 'Consistency Decisions'). The EDPB also advises the European Commission on any issue related to the protection of personal data and new proposed legislation in the European Union.

The Board acts in accordance with its [rules of procedure](#) and [guiding principles](#).

The EDPB is composed of representatives of the national data protection authorities and the European Data Protection Supervisor (EDPS). The Supervisory Authorities of the EFTA EEA States (Iceland, Liechtenstein and Norway) are also members with regard to GDPR-related matters, although they do not hold the right to vote nor can they be elected as chair or deputy chair. The European Commission and – with regard to GDPR-related matters – the European Free Trade



Association (EFTA) Surveillance Authority have the right to participate in the activities and meetings of the Board, but without voting rights.



The EDPB has a [Secretariat](#), which is provided by the EDPS. A [Memorandum of Understanding](#) determines the terms of cooperation between the EDPB and the EDPS. This Memorandum was signed during the first plenary meeting of the European Data Protection Board on 25 May 2018.



# 3



## 2018 Setting up of the EDPB and the Secretariat – an overview

The [rules of procedure](#) were adopted during the first plenary meeting of the European Data Protection Board, which took place on 25 May 2018. Several modifications were approved on 23 November 2018.

To assist in performing its tasks, several **expert subgroups** were set up within the EDPB. In addition, the **EDPB Secretariat** was established to provide analytical, administrative and logistical support to the EDPB.

### 3.1. EDPB'S ACTIVITIES

Between 25 May and 31 December 2018, the EDPB held **five plenary sessions**. In addition, there were 36 subgroup meetings.

During its first plenary meeting on 25 May 2018, the EDPB **endorsed 16 Guidelines** previously established by the Article 29 Working Party (WP29). During the remainder of 2018, the EDPB adopted **four more Guidelines** that aim

to clarify a range of provisions under the GDPR. These Guidelines addressed certification and the identification of certification criteria, derogations relating to international transfers, the territorial scope of the GDPR and the accreditation of certification bodies.

To guarantee the consistent application of the GDPR in cases where a competent Supervisory Authority wants to adopt specific measures having cross-border implications, the EDPB issues **Consistency Opinions**. The competent Supervisory Authority has to take utmost account of the opinion. Between 25 May and 31 December 2018, 26 Opinions on the national lists of processing operations subject to a Data Protection Impact Assessment (DPIA) were adopted by the EDPB. The purpose of the exercise was to ensure consistency across all national lists.

The EDPB also acts as a dispute resolution body and issues **binding decisions**. From 25 May to 31 December



2018, however, no dispute resolutions were initiated. This suggests that, to date, Supervisory Authorities have been able to reach consensus on all current cross border cases.

The EDPB **advises the European Commission** on any issue related to the protection of personal data, including assessments of the standard of data protection in third countries or international organisations. In 2018, the EDPB issued two such Opinions, at the request of the Commission: one on electronic evidence (e-Evidence) and one on the EU-Japan draft adequacy decision. On its own initiative, the EDPB also adopted a statement on economic concentration.

In 2018, the EDPB also adopted two **letters**, the first providing guidance to the Internet Corporation for Assigned Names and Numbers (ICANN) on how to develop a GDPR-compliant model for access to personal data processed in the context of their WHOIS system and the second relating to the revised Payments Services Directive (PSD2 Directive).

### **3.2. SUPERVISORY AUTHORITIES' ACTIVITIES**

Under the GDPR, the Supervisory Authorities have a duty to cooperate in order to ensure consistent application of the Regulation on **cases with a cross-border component**. Different cooperation procedures exist such as joint operations, mutual assistance, or a specific cooperation procedure labelled “One-Stop-Shop”.

Between 25 May and 31 December 2018, 255 cases with a cross-border component were registered in the IMI system. Most of the cases derived from complaints by individuals (176 cases). The rest (79 cases) originated from other sources. The three main topics of these cases related to data subjects’ rights, consumer rights, and data breaches.

In 2018, 43 **One-Stop-Shop procedures** were initiated by SAs from 14 different EEA countries. At the end of the year, the procedures were at different stages: 20 were at the informal consultation level, 20 were at draft decision level and two were final decisions. These first One-Stop-Shop final decisions related to the exercise of the rights of individuals, the appropriate legal basis for data processing and data breach notifications.

The **mutual assistance procedure** allows for Supervisory Authorities to ask for information from other SAs, but also to request other measures for effective cooperation. In the period between 25 May and 31 December 2018, 397 mutual assistance requests, both formal and informal, were triggered. 89% of the requests were replied to within 23 days.

No **joint operations** were initiated in 2018.

In 2018, the Supervisory Authorities of the 31 EEA countries reported over a hundred thousand cases at the national level. The majority of cases were either related to complaints or were initiated on the basis of data breach notifications from controllers.

### **3.3. CONSULTATIONS**

The EDPB organises **public consultations** on its guidelines to gather the views and concerns of all interested stakeholders and citizens. In 2018, the EDPB issued three consultations on its draft Guidelines, respectively on certification, on the territorial scope of the GDPR and on the accreditation of certification bodies.

As part of the annual review of the EDPB activities – established by Article 71 of the GDPR – a **stakeholder survey** was conducted, focusing on 20 GDPR guidelines. Respondents were part of trade associations from Europe, North-America and Asia-Pacific.

Sixty-five percent of stakeholders considered the Guidelines to be useful. While 45 percent considered them to be sufficiently pragmatic and operational for their needs, 23 percent called for improvement. For instance, shorter and more pragmatic guidance was recommended.

The majority of feedback concerning the consulting and drafting process of the Guidelines was positive or neutral. Some stakeholders encouraged the EDPB to increase opportunities to be involved and cooperate in the drafting of Guidelines.

# 4

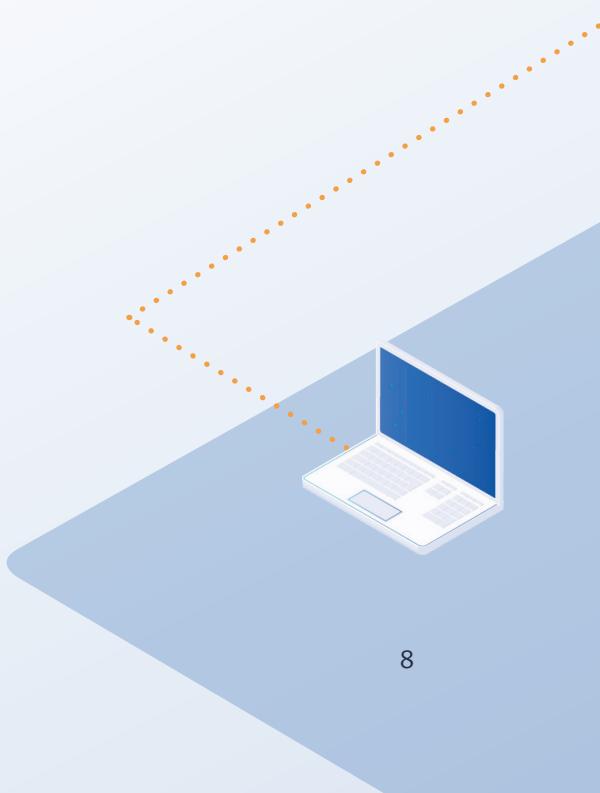


## Main objectives for 2019

In 2019 and 2020, the EDPB aims to focus on data subjects' rights, the concept of the controller and processor and legitimate interest in the guidance that it provides. The EDPB will continue to advise the Commission on matters such as cross-border data access requests for e-Evidence, the revision or introduction of adequacy decisions for data transfers to third countries and any possible revision of the

EU-Canada Passenger Name Record (PNR) agreement.

In 2019, the EDPB will continue its mission by deepening existing stakeholder relationships and developing new ones with relevant parties, while also continuing to participate in relevant conferences and maintaining a strong social media presence.



# Contact details

## **Postal address**

Rue Wiertz 60, B-1047 Brussels

## **Office address**

Rue Montoyer 30, B-1000 Brussels

## **Email**

[edpb@edpb.europa.eu](mailto:edpb@edpb.europa.eu)

 @eu\_edpb

 eu-edpb

 edpb.europa.eu



European Data Protection Board

# 2019 ANNUAL REPORT

# WORKING TOGETHER FOR STRONGER RIGHTS

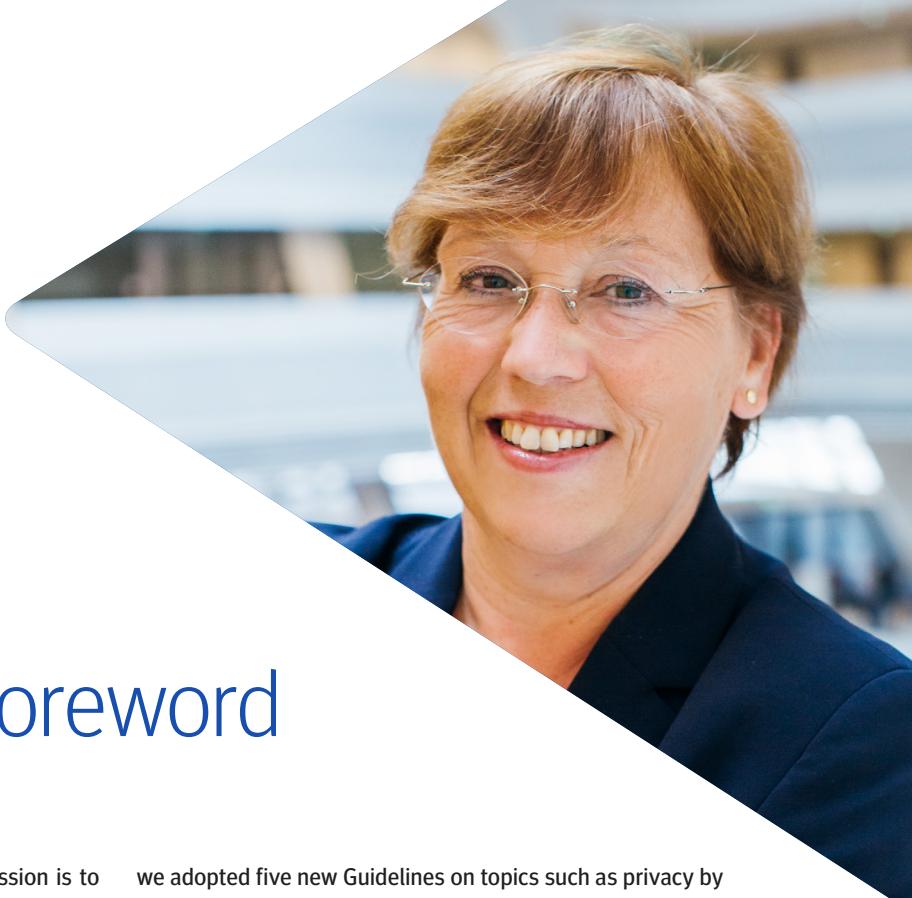
## EXECUTIVE SUMMARY



European Data Protection Board  
2019 Annual Report Executive Summary

**WORKING TOGETHER  
FOR STRONGER RIGHTS**

Further details about the EDPB can be found on our website at [edpb.europa.eu](http://edpb.europa.eu).



# Foreword

The European Data Protection Board's (EDPB) mission is to ensure the consistent application of data protection rules across the European Economic Area (EEA). This is enshrined in the General Data Protection Regulation (GDPR), which has opened the door to a new era of respect for data subject rights.

The GDPR is not just valuable insofar as it has established a harmonised legal framework for data protection across the EEA – one that has expanded and strengthened national data protection authorities' powers. The GDPR's entry into force has also encouraged greater awareness of data protection rights among individuals and organizations alike. This is more important than ever, given the increasing presence of data-dependent technologies in almost every facet of our lives.

As we approach the two-year anniversary of the GDPR's entry into application, I am convinced that the cooperation between EEA DPAs will result in the emergence of a common data protection culture. Some challenges remain, but the EDPB is working on solutions to overcome these and to make sure that the key cooperation procedure concepts are applied consistently.

As the EDPB, we contribute to the consistent interpretation of the GDPR by adopting Guidelines and Opinions. In 2019,

we adopted five new Guidelines on topics such as privacy by design and default, and the right to be forgotten, as well as two Guidelines in their final, post-consultation versions. We also adopted 16 Consistency Opinions covering, among other topics, Data Protection Impact Assessments, accreditation requirements for code of conduct monitoring bodies, and the interplay between the ePrivacy Directive and the GDPR.

This was possible thanks to the consistent efforts of all actors within the EDPB, as well as the increased input and engagement from our stakeholders via events, workshops and surveys.

As we look forward to the coming year, we feel ready to tackle the outstanding items in our two-year working programme. We will continue to adopt guidance, to promote the cooperation on cross-border enforcement, and to advise the EU legislator on data protection issues.

More and more countries outside the EU are adopting data protection legislation. In doing so, they often base their legislation on the fundamental principles of the GDPR. I am confident that, in a not too distant future, we will see the protection of data subject rights become a global norm. This will lay the foundation for more secure data flows and increased transparency, as well as improved trust in the rule of law.

**Andrea Jelinek**  
**Chair of the European Data Protection Board**

# 2



## 2019 – an overview

### 2.1. RULES OF PROCEDURE

The [Rules of Procedure \(RoP\)](#), which outline the EDPB's most important operational rules, were adopted during the first plenary meeting on 25 May 2018.

In 2019, the EDPB adopted revised wording for Articles 8, 10, 22 and 24 of its RoP, aimed at clarifying requirements to be granted observer status, procedures following the adoption of Opinions, and voting procedures during EDPB's plenary meetings.

The EDPB also adopted a new Article 37 RoP establishing a Coordinated Supervision Committee in the context of data processing by large information systems in use within the EU institutions, as well as by EU bodies, offices and agencies.

In 2019, the Committee was in charge of the coordinated supervision of the IMI system and Eurojust. In 2020, this will be extended to include the European Public Prosecutor Office (EPPO). In the future, all coordinated supervision of large EU information systems, bodies, offices and agencies will gradually be moved to the Committee.

### 2.2. THE EDPB SECRETARIAT

The EDPB Secretariat ensures that all of the EDPB's activities comply with the legal framework applicable to the EDPB as an EU body and with its RoP. It is the main drafter for Consistency Opinions and Decisions, and serves as an institutional memory, ensuring documents' consistency over time. The role of the EDPB Secretariat is also to facilitate the EDPB's fair and effective decision-making and to act as a gateway for clear and consistent communication.

As part of its support activities, the EDPB Secretariat has developed IT solutions to enable effective and secure communication between the EDPB members, including the Internal Market Information System (IMI).

In 2019, the EDPB Secretariat organised 11 plenary meetings and 90 expert subgroup meetings. The different expert subgroups focus on specific areas of data protection and assist the EDPB in performing its tasks.

Finally, the EDPB Secretariat assists the Chair in preparing for and presiding over the plenary meetings, as well with her speaking engagements.

### 2.3. EDPB ACTIVITIES IN 2019

#### 2.3.1. General Guidance

In 2019, the EDPB adopted [five new Guidelines](#) aimed at clarifying the range of provisions under the GDPR. The adopted Guidelines addressed codes of conduct and monitoring bodies at a national and European level, as well as clarifying the processing of personal data under a range of circumstances, namely during the provision of online services, through video devices, on the principles of Data Protection by Design & Default, and related to the Right to be Forgotten by search engines.

In addition, [three Guidelines](#) adopted in 2018 were approved by the EDPB in their final form in 2019, following public consultations. These Guidelines clarify accreditation and certification criteria and the territorial scope outlined in the GDPR.

The EDPB also issued a [recommendation](#) on the draft list submitted by the EDPS on processing operations which require a Data Protection Impact Assessment (DPIA).

#### 2.3.2. Consistency Opinions

To guarantee the consistent application of the GDPR in cases with cross-border implications, the EDPB issues Consistency Opinions. The competent SA has to take utmost account of the opinion.

In 2019, the EDPB adopted [16 Consistency Opinions](#). Eight of these concerned the draft lists submitted by SAs on processing operations requiring a DPIA, as well as those exempt from it. The remaining Opinions regarded transfers of personal data between EEA and non-EEA Financial SAs and the interplay between the ePrivacy Directive and the GDPR, as well as clarifying Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), SAs' competences, and Accreditation Criteria for monitoring bodies.

The EDPB also acts as a dispute resolution body and issues [binding decisions](#). Since 25 May 2018, however, no dispute resolutions have been initiated. This suggests that, to date, SAs have been able to reach consensus on all current cross-border cases.

#### 2.3.3. Legislative consultation

The EDPB advises the European Commission on any issue related to the protection of personal data, including the adequacy of the level of data protection in third countries or international organisations. In 2019, the EDPB issued reports on the [Second](#) and [Third Annual Review](#) of the EU-U.S. Privacy Shield adequacy decision, conducted by the European Commission to assess its robustness and practical implementation.

In addition, the EDPB issued an [Opinion](#) on the interplay between the Clinical Trials Regulation (CTR) and the GDPR, requested by the European Commission's Directorate-General for Health and Food Safety (DG SANTE).

The EDPB is also subject to Article 42 of [Regulation 2018/1725](#) on legislative consultation. This allows the EDPS and the EDPB to coordinate their work with a view to issuing a [Joint Opinion](#). In 2019, the EDPB and the EDPS adopted a [Joint Opinion](#) concerning the data protection aspects of the eHealth Digital Service Infrastructure. This Opinion was also issued following DG SANTE's request.

The EDPB also adopted, on its own initiative, a [statement](#) on the draft ePrivacy Regulation and issued a [contribution](#) on the data protection aspects of the Budapest Convention on Cybercrime.

#### 2.3.4. Other documents

In 2019, the EDPB adopted **two statements**. The [first one](#) concerned the US Foreign Account Tax Compliance Act (FATCA), following the European Parliament's resolution on the adverse effects of the FATCA on EU citizens. The [second one](#) regarded use of personal data in the course of political campaigns, in light of the 2019 European Parliament elections and other elections taking place across the EU and beyond.

To address issues of data protection in the event of a no-deal Brexit, the EDPB adopted **two information notes**, on [data transfers](#) from the EEA to the UK under the GDPR, and on [BCRs for companies](#) having the UK Information Commissioner's Office as Lead SA.

Following a request made by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs Committee (LIBE), the EDPB issued the [LIBE report on the implementation of GDPR](#), providing an overview of the implementation and enforcement of the GDPR covering both the cooperation mechanism and the consistency findings.

On 9 July 2019, the EDPB Chair pleaded before the Court of Justice of the European Union, which had requested an oral [pleading on Case C-311/18 \(Facebook Ireland and Schrems\)](#).

#### 2.4. CONSULTATIONS

Following the preliminary adoption of Guidelines, the EDPB organises **public consultations** to allow stakeholders and citizens to share their views and provide additional input. In 2019, the EDPB launched [five such consultations](#), concerning its Guidelines on Codes of Conduct, Certification Criteria, processing of personal data in online services and video devices, Data Protection by Design and Default, and the Right to be Forgotten.

The EDPB organises **stakeholder events** to gather views on key issues and to inform the development of future guidance.

In 2019, the EDPB organised three such events focused on the revised Payments Services Directive (PSD2), on the concepts and responsibilities of controllers and processors, and on data subject rights.

As part of the annual review of the EDPB activities – established by Article 71.2 GDPR – the EDPB conducted a **stakeholder survey** for the second year in a row. The survey, which focused on the content and adoption process of the EDPB's Guidelines, aimed to understand to what extent stakeholders find the guidelines helpful and practical in interpreting the GDPR's provisions.

Respondents included organisations and individual companies from the financial, banking and insurance sectors, wholesale and retail trade, information technologies, human health and social work activities and fundamental rights. The majority of respondents were based in Europe, and over 60 percent represented small entities.

64 percent of stakeholders who participated in the survey found the Guidelines to be useful, while 46 percent considered them to be sufficiently pragmatic. Nearly 80 percent found the Guidelines easily accessible; this was up from 64 percent in 2018. Other positive feedback referenced the Guidelines' real-life examples and wide applicability preventing national fragmentation.

Respondents encouraged further interpretative work to clarify, among other things, the relationship between controller and processor and the legal basis of legitimate interest. Compliance with the GDPR for SMEs remains a challenge, but stakeholders noted that the EDPB's Guidelines are a useful tool in supporting its application. Overall, 40 percent of stakeholders classified the consultative process as ranging from appropriate to satisfying.

#### 2.5. SUPERVISORY AUTHORITIES ACTIVITIES IN 2019

Under the GDPR, the European Economic Area (EEA) Member States' SAs cooperate closely to ensure that individuals' data protection rights are protected consistently across the EEA. One task for the SAs is to assist one another and coordinate decision-making in cross-border data protection cases.

During the reporting period, SAs identified certain challenges when implementing the cooperation and consistency mechanism. In particular, the patchwork of national procedural laws was found to have an impact on the cooperation mechanism, due to differences in complaint handling procedures, position of the parties in the proceedings, admissibility criteria, duration of proceedings, deadlines, etc.

In addition, SAs' effective application of the powers and tasks attributed to them by the GDPR depends largely on the resources they have available. This applies in particular to the One-Stop-Shop (OSS) mechanism, the success of which is contingent on the time and effort SAs can dedicate to individual cases and cooperation.

Despite these challenges, the EDPB is convinced that the cooperation between SAs will result in a common data protection culture and consistent monitoring practices. One single set of rules has proved to be advantageous for data controllers and processors within the EEA, having brought greater legal certainty. It has also benefitted individuals who have seen their data subject rights reinforced.

Since the entry into application of the GDPR, there have been 807 cross-border cooperation procedures in the IMI system, out of which 585 cases were started in 2019. Of these cross-border cooperation procedures, 425 resulted from a complaint, while the remaining originated from other sources, such as investigations, legal obligations or media reports.

The **OSS mechanism** demands cooperation between the Lead Supervisory Authority (LSA) and the Concerned Supervisory Authorities (CSAs). The LSA leads the investigation and plays a key role in the process of reaching consensus between the CSAs, in addition to working to reach a coordinated decision with regard to the data controller or processor. By the end of 2019, 142 OSS procedures were initiated by SAs, 79 of which resulted in a final decision.

The **mutual assistance procedure** allows SAs to ask for information from other SAs or to request other measures for effective cooperation, such as prior authorisations or

investigations. Since 25 May 2018, 2,542 mutual assistance procedures have been triggered. Of these procedures, the overwhelming majority (2,427) were informal consultation procedures, while 115 were formal requests.

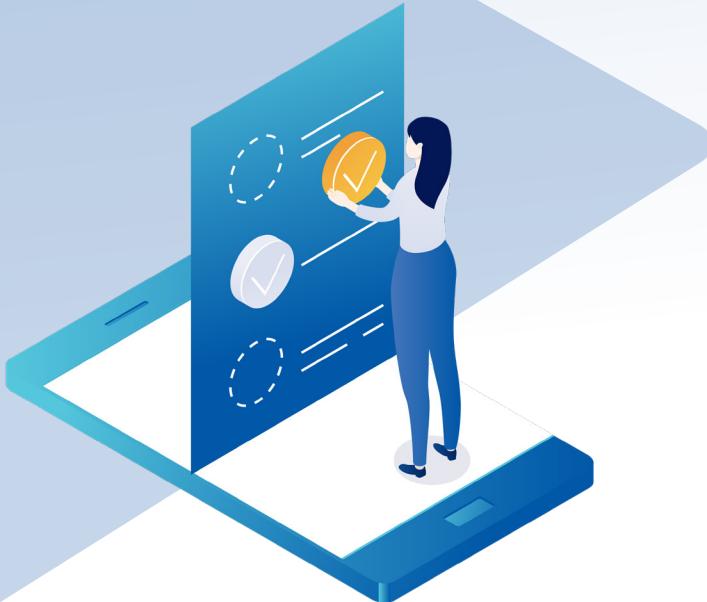
In 2019, **no joint operations** were carried out by SAs.

Under the GDPR, national SAs have different corrective measures at their disposal. In 2019, SAs identified a number of **violations of the GDPR** and exercised their corrective powers accordingly.

Violations included failure to implement provisions such as privacy by default and design, right to access or right to erasure. Many cases highlighted a lack of proper technical and organisational measures for ensuring data protection, which led to data breaches. Several significant incidents involved the processing of special categories of data, such as political opinions, credit information or biometric data. The entities fined were from both the private and the public sector.



# 3



## Main objectives for 2020

By the end of 2019, halfway through its [work plan](#), the EDPB had made significant progress across its stated objectives and is advancing towards completing them in its second working year.

In 2020, the EDPB will aim to provide guidance on data controllers and processors, data subject rights and the concept of legitimate interest. It will also intensify its work in the context of advanced technologies, such as connected vehicles, blockchain, artificial intelligence, and digital assistants.

The EDPB will continue to advise the European Commission on issues such as cross-border e-Evidence data access requests, the revision or adoption of adequacy decisions for data transfers to third countries, and any possible revision of the EU-Canada Passenger Name Record (PNR) agreement.

In addition to the work outlined in the work plan, in 2020, the EDPB is to provide guidance on the implications for

data protection in the context of the fight against COVID-19, both at its own initiative and upon consultation by the European Commission.

The EDPB is also committed to deepening existing stakeholder relationships and developing new ones. The EDPB Members, as well as the EDPB Chair and Deputy Chairs, will continue participating in relevant conferences and speaking engagements.

The EDPB Secretariat will continue to ensure a harmonised communication approach. This includes continuing to drive public engagement with the EDPB's activities through its social media presence, as well as enhancing cooperation with SAs. To this end, the EDPB will maintain and strengthen the network of SAs' press and communications officers.



# Contact details

**Postal address:**

Rue Wiertz 60, B-1047 Brussels

**Office address:**

Rue Montoyer 30, B-1000 Brussels

**Email:**

[edpb@edpb.europa.eu](mailto:edpb@edpb.europa.eu)

-  @eu\_edpb
-  eu-edpb
-  edpb.europa.eu



European Data Protection Board

# 2019 ANNUAL REPORT

## WORKING TOGETHER FOR STRONGER RIGHTS



European Data Protection Board  
2019 Annual Report

# WORKING TOGETHER FOR STRONGER RIGHTS

An Executive Summary of this report, which provides an overview of key EDPB activities in 2019, is also available.

Further details about the EDPB can be found on our website at [edpb.europa.eu](http://edpb.europa.eu).

# TABLE OF CONTENTS

<b>1</b>	<b>FOREWORD</b>	<b>4</b>
<b>2</b>	<b>MISSION STATEMENT, TASKS AND PRINCIPLES</b>	<b>5</b>
<b>2.1.</b>	Tasks and duties	5
<b>2.2.</b>	Guiding principles	6
<b>3</b>	<b>ABOUT THE EUROPEAN DATA PROTECTION BOARD</b>	<b>7</b>
<b>4</b>	<b>2019 - AN OVERVIEW</b>	<b>8</b>
<b>4.1.</b>	Functioning of the EDPB: revised rules of procedure	8
4.1.1.	Article 8 RoP: Observers	8
4.1.2.	Article 10 RoP: Opinions of the Board under Article 64 GDPR	8
4.1.3.	Article 22 RoP: Voting procedure	9
4.1.4.	Article 24 RoP: Written voting procedure	9
4.1.5.	Article 37 RoP: Establishing the Coordinated Supervision Committee	9
<b>4.2.</b>	The EDPB Secretariat	10
<b>4.3.</b>	Cooperation and consistency	10
4.1.3.	IT communications tool (IMI)	11
<b>5</b>	<b>EUROPEAN DATA PROTECTION BOARD ACTIVITIES IN 2019</b>	<b>12</b>
<b>5.1.</b>	General guidance	12
5.1.1.	Guidelines on Code of Conduct	13
5.1.2.	Guidelines on the processing of personal data in the context of online services	13
5.1.3.	Recommendation on the EDPS draft list on processing operations subject to Data Protection Impact Assessments (DPIAs)	13
5.1.4.	Guidelines on processing of personal data through video services	14
5.1.5.	Guidelines on Data Protection by Design and by Default	14
5.1.6.	Guidelines on the Right to be Forgotten	15
5.1.7.	Guidelines adopted following public consultation	15
<b>5.2.</b>	Consistency Opinions	15
5.2.1.	Opinions on the draft Data Protection Impact Assessments lists (DPIAs)	16
5.2.2.	Opinion on transfers of personal data between EEA and non-EEA Financial Supervisory Authorities	16
5.2.3.	Opinion on the interplay between ePrivacy Directive and the GDPR	16
5.2.4.	Opinion on the competence of a Supervisory Authority in case of a change in circumstances relating to the main or single establishment	16
5.2.5.	Opinions on Accreditation Criteria for monitoring bodies of Code of Conduct	17
5.2.6.	Opinion on Standard Contractual Clauses for processors by Danish SA	17
5.2.7.	Opinions on Binding Corporate Rules	18
<b>5.3.</b>	Legislative consultation	18
5.3.1.	EU-U.S. Privacy Shield	18
5.3.2.	Opinion on clinical trials Q&A	19
5.3.3.	Statement on the future ePrivacy regulation	19
5.3.4.	Additional protocol to the Budapest Convention on Cybercrime	19
5.3.5.	EDPB-EDPS Joint Opinion on the eHealth Digital Service Infrastructure	20
<b>5.4.</b>	Other documents	20
5.4.1.	Information note on data transfers under the GDPR in the event of a no-deal Brexit	20
5.4.2.	Information note on Binding Corporate Rules for companies which have the UK Information Commissioner's Office as BCR Lead Supervisory Authority	20
5.4.3.	Statement on the US Foreign Account Tax Compliance Act	20
5.4.4.	Statement on the use of personal data in political campaigns	21
5.4.5.	LIVE Report on the implementation of the GDPR	21
5.4.6.	EDPB pleading before the CJEU in Case C-311/18 (Facebook Ireland and Schrems)	22
<b>5.5.</b>	Plenary meetings and subgroups	22
<b>5.6.</b>	Stakeholder consultations and transparency	23
5.6.1.	Stakeholder events on future guidance	23
5.6.1.1.	Interplay of PSD2 and GDPR	23
<b>6.</b>	<b>SUPERVISORY AUTHORITY ACTIVITIES IN 2019</b>	<b>28</b>
<b>6.1.</b>	Cross-border cooperation	28
6.1.1.	Preliminary procedure to identify the Lead and Concerned Supervisory Authorities	28
6.1.2.	Database regarding cases with cross-border component	29
6.1.3.	One-Stop-Shop Mechanism	29
6.1.4.	Mutual assistance	30
6.1.5.	Joint operations	31
<b>6.2.</b>	National cases	31
6.2.1.	Some relevant national cases with exercise of corrective powers	31
6.2.1.1.	Austria	31
6.2.1.2.	Belgium	31
6.2.1.3.	Denmark	32
6.2.1.4.	Finland	32
6.2.1.5.	France	32
6.2.1.6.	Germany	33
6.2.1.7.	Greece	33
<b>7.</b>	<b>COORDINATED SUPERVISION COMMITTEE OF THE LARGE-SCALE EU INFORMATION SYSTEMS AND OF EU BODIES, OFFICES AND AGENCIES</b>	<b>38</b>
<b>8.</b>	<b>MAIN OBJECTIVES FOR 2020</b>	<b>40</b>
<b>8.1.</b>	Legal work plan	40
8.1.1.	Guidance	40
8.1.2.	Advisory role to the European Commission	40
8.1.3.	Consistency findings	41
<b>8.2.</b>	Communications	41
<b>9.</b>	<b>ANNEXES</b>	<b>42</b>
<b>9.1.</b>	General guidance adopted in 2019	42
<b>9.2.</b>	Consistency Opinions adopted in 2019	42
<b>9.3.</b>	Joint Opinions adopted in 2019	43
<b>9.4.</b>	Legislative consultation	43
<b>9.5.</b>	Other documents	43
<b>9.6.</b>	List of expert subgroups with scope of mandate	44



# Foreword

The European Data Protection Board's (EDPB) mission is to ensure the consistent application of data protection rules across the European Economic Area (EEA). This is enshrined in the General Data Protection Regulation (GDPR), which has opened the door to a new era of respect for data subject rights.

The GDPR is not just valuable insofar as it has established a harmonised legal framework for data protection across the EEA – one that has expanded and strengthened national data protection authorities' powers. The GDPR's entry into force has also encouraged greater awareness of data protection rights among individuals and organizations alike. This is more important than ever, given the increasing presence of data-dependent technologies in almost every facet of our lives.

As we approach the two-year anniversary of the GDPR's entry into application, I am convinced that the cooperation between EEA DPAs will result in the emergence of a common data protection culture. Some challenges remain, but the EDPB is working on solutions to overcome these and to make sure that the key cooperation procedure concepts are applied consistently.

As the EDPB, we contribute to the consistent interpretation of the GDPR by adopting Guidelines and Opinions. In 2019,

we adopted five new Guidelines on topics such as privacy by design and default, and the right to be forgotten, as well as two Guidelines in their final, post-consultation versions. We also adopted 16 Consistency Opinions covering, among other topics, Data Protection Impact Assessments, accreditation requirements for code of conduct monitoring bodies, and the interplay between the ePrivacy Directive and the GDPR.

This was possible thanks to the consistent efforts of all actors within the EDPB, as well as the increased input and engagement from our stakeholders via events, workshops and surveys.

As we look forward to the coming year, we feel ready to tackle the outstanding items in our two-year working programme. We will continue to adopt guidance, to promote the cooperation on cross-border enforcement, and to advise the EU legislator on data protection issues.

More and more countries outside the EU are adopting data protection legislation. In doing so, they often base their legislation on the fundamental principles of the GDPR. I am confident that, in a not too distant future, we will see the protection of data subject rights become a global norm. This will lay the foundation for more secure data flows and increased transparency, as well as improved trust in the rule of law.

**Andrea Jelinek**  
**Chair of the European Data Protection Board**

# 2



## Mission statement, tasks and principles

The European Data Protection Board (EDPB) aims to ensure the consistent application of the [General Data Protection Regulation](#) (GDPR) and of the [European Law Enforcement Directive](#) across the European Economic Area (EEA).

The EDPB can adopt general guidance to further clarify European data protection laws, giving stakeholders, including individuals, a consistent interpretation of their rights and obligations as well as providing Supervisory Authorities (SAs) with a benchmark for enforcing the GDPR.

The EDPB is also empowered to issue Opinions or Decisions (more precisely, ‘Consistency Opinions’ or ‘Consistency Decisions’) to guarantee a consistent application of the GDPR by SAs across the EEA.

The EDPB acts in accordance with its [rules of procedure](#) and [guiding principles](#).

### 2.1. TASKS AND DUTIES

- The EDPB provides [general guidance](#) (including guidelines, recommendations and best practices) to clarify the law.
- The EDPB issues **Consistency** Opinions or Decisions to guarantee the consistent application of the GDPR by the EEA SAs.
- The EDPB promotes **cooperation** and the effective exchange of information and best practices between national SAs.
- The EDPB **advises** the European Commission on any issue related to the protection of personal data and new proposed legislation in the European Union.

### 2.2. GUIDING PRINCIPLES

- **Independence and impartiality.** The EDPB is an independent body, which performs its tasks and exercises its powers impartially.
- **Good governance, integrity and good administrative behaviour.** The EDPB acts in the public interest as an expert, trustworthy and authoritative body in the field of data protection, with good decision-making processes and sound financial management.
- **Collegiality and inclusiveness.** The EDPB is organised and acts collectively as a collegiate body, as established by the provisions of the GDPR and the European Law Enforcement Directive.
- **Cooperation.** The EDPB promotes cooperation between SAs and endeavours to operate by consensus wherever possible, holding the GDPR and the European Law Enforcement Directive as an overarching reference.
- **Transparency.** The EDPB carries out its work as openly as possible, so as to be more effective and more accountable to the public. The EDPB strives to explain its activities using clear language that is accessible to all.
- **Efficiency and modernisation.** The EDPB makes every effort to ensure that its work is as efficient and as flexible as possible, in order to achieve the highest level of cooperation between its members. The EDPB does this by using new technologies to keep working methods up to date, minimise formalities, and provide efficient administrative support.
- **Proactivity.** The EDPB undertakes its own initiatives, in order to anticipate and support innovative solutions that will help overcome digital challenges to data protection. The EDPB encourages the effective participation of stakeholders (whether members, observers, staff or invited experts), so that their needs and aspirations can be fully taken into account.

# 3



## About the European Data Protection Board

The European Data Protection Board (EDPB) is an independent European body, which contributes to the consistent application of data protection rules throughout the European Economic Area (EEA) and promotes cooperation between the EEA Supervisory Authorities (SAs).

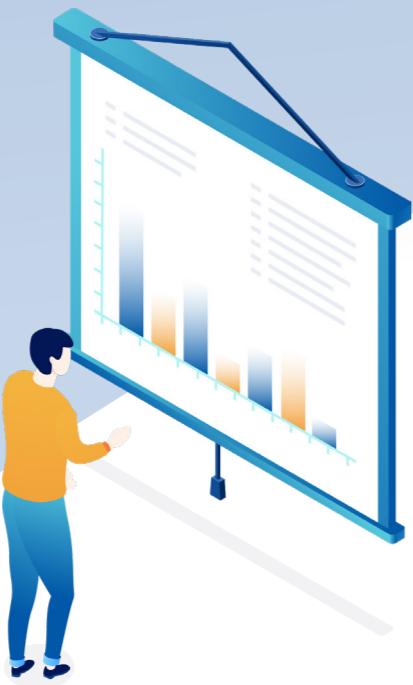
The EDPB is composed of representatives of the SAs and the European Data Protection Supervisor (EDPS). The SAs of the EEA/EFTA (European Free Trade Association) States (Iceland, Liechtenstein and Norway) are also members with regard to GDPR-related matters, although they do not hold the right to vote, nor can they be elected as Chair or Deputy Chair of the EDPB.

The EDPB was established by the [General Data Protection Regulation \(GDPR\)](#). The European Commission and – with regard to GDPR-related matters – the EFTA Surveillance Authority have the right to participate in the activities and meetings of the EDPB without voting rights.

The EDPB has a [Secretariat \(the EDPB Secretariat\)](#), which is provided by the EDPS. A [Memorandum of Understanding](#) determines the terms of cooperation between the EDPB and the EDPS.



# 4



## 2019 – an overview

### 4.1. FUNCTIONING OF THE EDPB: REVISED RULES OF PROCEDURE

The [Rules of Procedure](#) (RoP) were adopted during the first plenary meeting of the EDPB on 25 May 2018. These outline the EDPB's most important operational rules, describing:

- The EDPB's guiding principles;
- The organisation of the EDPB;
- The cooperation between the EDPB members;
- The election of the Chair and the Deputy Chair of the EDPB;
- The EDPB's working methods.

In 2019, the EDPB adopted revised wording for Articles 8, 10, 22 and 24 of its RoP. The EDPB also adopted a new Article 37 RoP establishing a Coordinated Supervision Committee in the

context of data processing by large information systems in use within the EU institutions, as well as by EU bodies, offices and agencies.

#### 4.1.1. Article 8 RoP: Observers

Article 8 RoP outlines the possibility for the EDPB to have observers. In 2019, new wording was adopted to clarify the requirements for a non-EU country's data protection authority to be granted observer status.

#### 4.1.2. Article 10 RoP: Opinions of the Board under Article 64 GDPR

The revision of Article 10 RoP clarified the procedure that follows the adoption of a Consistency Opinion under Article 64 GDPR.

The adopted changes ensure that all EDPB members will be informed whether an SA intends to maintain or amend its draft decision following the EDPB's Opinion.

In addition, the EDPB Secretariat, the rapporteurs and the expert subgroup members who prepared the Opinion will inform the EDPB members and the European Commission about how, in their view, the SA's amended decision takes into account the EDPB's Opinion. This provides both the EEA SAs and the EDPB with valuable feedback and enables them to exercise their rights under Article 65.1.c GDPR.

The revised article also encompasses any situation where an SA indicates to the EDPB Chair that it will not follow the Opinion of the EDPB, whether in part or as a whole. In this case, the RoP enable the Chair and the Deputy Chairs of the EDPB to refer the matter to the EDPB under Article 65.1.c GDPR. This does not, however, affect the right of any other concerned SA, of the European Commission or of the EFTA Surveillance Authority to refer the matter to the EDPB for an Article 65 GDPR decision procedure.

Finally, the revised article makes clear that the EDPB will not adopt any Opinion or any other position in the context of the same Article 64 GDPR procedure, e.g. to confirm that the amended draft decision is in line with the adopted Opinion.

#### 4.1.3. Article 22 RoP: Voting procedure

In the updated version of the RoP, the EDPB clarified the voting procedures relating to its plenary meetings.

In particular, all votes on the final adoption of documents should be counted from the total number of EDPB members entitled to vote, regardless of whether they are present for the actual vote or not.

#### 4.1.4. Article 24 RoP: Written voting procedure

Revised Article 24 RoP raised the threshold necessary for the suspension of written procedures decided by the Chair of

the EDPB. According to the new text, at least three entitled-to-vote EDPB members are needed to request a suspension of the written procedure decided by the Chair of the EDPB.

In addition, the Chair of the EDPB will be able to suspend the written procedure decided by the EDPB upon the request of one EDPB member only if new circumstances that may substantially affect the outcome of the procedure arise.

**The EDPB updated Rules of Procedure establish a Coordinated Supervision Committee and clarify the role of observers and voting procedures.**

#### 4.1.5. Article 37 RoP: Establishing the Coordinated Supervision Committee

In October 2018, [Regulation 2018/1725](#) on the protection of personal data processed by the EU institutions and bodies was adopted. In accordance with Article 62 of this regulation, the European Data Protection Supervisor (EDPS) and the national SAs shall cooperate actively to ensure effective supervision of large-scale IT systems and of Union bodies, offices and agencies. As a result, the Coordinated Supervision Committee was created.

Consequently, the EDPB's RoP were amended to include a new Article 37, which formally establishes the Coordinated Supervision Committee within the EDPB. This Committee includes representatives from national SAs, the EDPS, and the SAs of non-EU Schengen Member States, when foreseen under EU law. The Rules of Procedure make clear that the participation in the Committee may differ from the EDPB's membership and participation. (For more information on the Committee, see Section 7.)

Article 37 RoP takes a horizontal and flexible approach to ensure consistent application and structure for the coordinated supervision of various EU information systems. The article establishes that the Committee functions autonomously with respect to the EDPB's activities, adhering to its own rules of procedure and working methods. The Secretariat of the Committee is provided by the EDPB Secretariat.

Article 37 RoP also requires the Committee to meet at least twice a year and to submit a joint report on coordinated supervision activities to the European Parliament, the European Council and the European Commission.

#### 4.2. THE EDPB SECRETARIAT

The EDPB Secretariat ensures that all of the EDPB's activities comply with the legal framework applicable to the EDPB as an EU body and with its RoP. It is the main drafter for Consistency Opinions and Decisions, and serves as an institutional memory, ensuring documents' consistency over time. The role of the EDPB Secretariat is also to facilitate the EDPB's fair and effective decision-making and to act as a gateway for clear and consistent communication.

As outlined in the GDPR, the EDPB Secretariat is provided by the EDPS, which is a member of the EDPB, and is required to perform all its tasks exclusively under the instructions of the Chair of the EDPB. The EDPB Secretariat deals with a range of tasks, from drafting legal documents to handling media relations and organizing meetings.

As part of its support activities, the EDPB Secretariat has developed IT solutions to enable effective and secure communication between the EDPB members, including the Internal Market Information System (IMI). It has also set up a network of communications officers within the SAs, to develop and implement shared communication on EDPB news, information campaigns and communication tools.

Finally, the EDPB Secretariat assists the Chair in preparing for and presiding over the plenary meetings, as well with her speaking engagements.

#### 4.3. COOPERATION AND CONSISTENCY

Under the GDPR, EEA Member States' SAs cooperate closely to ensure that individuals' data protection rights are protected consistently across the EEA. One task is to assist one another and coordinate decision-making in cross-border data protection cases.

Via the so-called cooperation and consistency mechanism, the EDPB issues Consistency Opinions or Decisions. In 2019, the EDPB adopted several Opinions and Guidelines (outlined in Section 5 of this report) to clarify fundamental provisions of the GDPR and to ensure consistency in its application among SAs.

The EDPB can also issue legally binding Consistency Decisions, for instance aiming to arbitrate if and when national SAs take different positions in cross-border cases.

SAs identified certain challenges when implementing the cooperation and consistency mechanism. In particular, the patchwork of national procedural laws was found to have an impact on the cooperation mechanism, due to differences in complaint handling procedures, position of the parties in the proceedings, admissibility criteria, duration of proceedings, deadlines, etc.

In addition, SAs' effective application of the powers and tasks attributed to them by the GDPR depends largely on the resources they have available. This applies in particular to the One-Stop-Shop (OSS) mechanism, the success of which is contingent on the time and effort SAs can dedicate to individual cases and cooperation.

Despite these challenges, the EDPB is convinced that the cooperation between SAs will result in a common data protection culture and consistent monitoring practices. One single set of rules has proved to be advantageous for data controllers and processors within the EEA, having brought greater legal certainty. It has also benefitted individuals who have seen their data subject rights reinforced.

The EDPB also promotes the cooperation between the EEA SAs in their task. The EDPB Secretariat provides logistical

support to some types of national cooperation taking place before any formal involvement of the EDPB. This will be applicable for the cooperation between SAs in case a competent SA prepares Binding Corporate Rules (BCR), Codes of Conduct or Certification Criteria.

The EDPB, upon the initiative of the EDPS, has also launched a secondment programme enabling staff exchanges between the EEA SAs and the EDPS, including the EDPB Secretariat.

#### 4.3.1. IT COMMUNICATIONS TOOL (IMI)

The EDPB promotes the cooperation between EEA SAs by providing a robust IT system. Since 25 May 2018, the SAs have been using the Internal Market Information (IMI) system to exchange information necessary for the GDPR cooperation and consistency mechanism in a standardised and secured way.

IMI is a system developed by the European Commission's Directorate General for Internal Market, Industry, Entrepreneurship and SMEs (DG GROW). It was adapted to cater for the needs of the GDPR, in close cooperation with the EDPB Secretariat and the SAs. Upon its adoption, IMI has

immediately proved to be an asset for SAs, which have since accessed and used the system on an almost daily basis.

To ensure that the IMI system is adapted to the changing needs of SAs, the EDPB created a dedicated expert subgroup which discusses and validates any necessary changes (i.e. a new workflow for the EDPB written procedure, available reports for different procedures, change of bilateral workflow of the information mutual assistance request into multilateral etc.). Additionally, the EDPB IMI Helpdesk has been created within the EDPB Secretariat, with dedicated staff providing day-to-day assistance to users.

Since the entry into application of the GDPR until the end of 2019, 807 cases were registered in the IMI system by the EEA SAs. From the case register, different procedures were initiated:

- Identification of the Lead Supervisory Authority (LSA) and Concerned Supervisory Authorities (CSA): 1,346 procedures.
- Mutual Assistance Procedures: 115 formal procedures and 2427 informal procedures.
- OSS: 142 draft decisions, out of which 79 resulted in final decisions.



# 5



## European Data Protection Board activities in 2019

The EDPB aims to ensure the consistent application of the [General Data Protection Regulation \(GDPR\)](#) and of the [European Law Enforcement Directive](#) across the European Economic Area (EEA).

The EDPB can adopt general guidance to clarify European data protection laws. This provides the public and stakeholders with a consistent interpretation of their rights and obligations, and ensures that Supervisory Authorities (SAs) have a benchmark for enforcing the GDPR.

The EDPB is also empowered to issue Opinions or Binding Decisions to guarantee the consistent application of the GDPR by national SAs.

### 5.1. GENERAL GUIDANCE

In 2019, the EDPB adopted five new Guidelines aimed at clarifying the range of provisions under the GDPR. Three were adopted in 2019 and finalised in the same year, following a public consultation. Two Guidelines were adopted in 2019 and subsequently submitted to public consultation. These had not yet been finalised by the end of 2019.

The adopted Guidelines addressed codes of conduct and monitoring bodies at a national and European level, as well as clarifying the processing of personal data under a range

of circumstances, namely during the provision of online services, through video devices, on the principles of Data Protection by Design & Default, and related to the Right to be Forgotten by search engines.

Three Guidelines adopted in 2018 were approved by the EDPB in their final form in 2019, following public consultations. These Guidelines clarify accreditation and certification criteria and the territorial scope outlined in the GDPR.

**Guidance provides stakeholders with a consistent interpretation of their rights and obligations.**

The EDPB also issued a recommendation on the draft list submitted by the European Data Protection Supervisor (EDPS) on processing operations which require a Data Protection Impact Assessment.

### 5.1.1. Guidelines on Codes of Conduct

During its seventh plenary meeting on 12 February 2019, the EDPB adopted the [Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679](#).

The aim of these Guidelines is to provide practical guidance and interpretative assistance in relation to the application of Articles 40 and 41 of the GDPR. They clarify the procedures and rules involved in the submission, approval and publication of codes of conduct at both national and European level.

These Guidelines should provide all competent SAs, the EDPB and the European Commission with a clear framework to evaluate codes of conduct in a consistent manner and to streamline the procedures involved in the assessment process.

A public consultation was launched following the adoption of the document. The final version of the Guidelines, including further points of clarification, was adopted on 4 June 2019.

### 5.1.2. Guidelines on the processing of personal data in the context of online services

On 9 and 10 April 2019, the EDPB met for its ninth plenary session. During this meeting, the EDPB adopted the [Guidelines 2/2019 on the processing of personal data under Article 6.1.b of the GDPR in the context of the provision of online services to data subjects](#). These Guidelines aim to clarify the scope and application of Article 6.1.b GDPR on lawfulness of processing, in the context of information society services.

The Guidelines make general observations regarding data protection principles and the interaction of Article 6.1.b GDPR with other lawful bases. In addition, they contain guidance on the applicability of Article 6.1.b GDPR in the context of bundling of separate services and termination of contract.

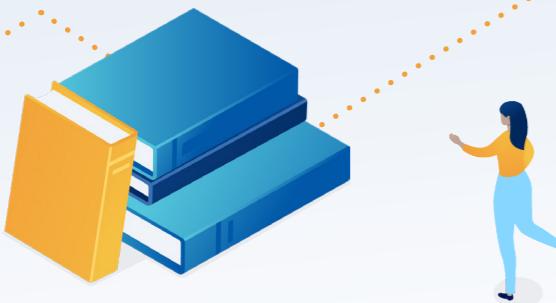
The document was subject to a public consultation. The final version of the Guidelines was adopted on 8 October 2019.

### 5.1.3. Recommendation on the EDPS draft list on processing operations subject to Data Protection Impact Assessments (DPIAs)

During its twelfth plenary meeting held on 9 and 10 July 2019, the EDPB adopted the [Recommendation 1/2019 on the draft list of the EDPS regarding the processing operations subject to the requirement of a Data Protection Impact Assessment](#).

Article 39.4 of [Regulation 2018/1725](#) requires the EDPS to establish and make public a list of the kind of processing operations which require a DPIA, with the goal of informing data controllers.

The EDPS has to consult with the EDPB prior to adoption of



these lists, since they refer to processing operations by a controller acting jointly with one or more controllers other than EU institutions and bodies.

In its Recommendation, the EDPB invited the EDPS to amend certain wording and examples around sensitive data, large-scale data processing, combined datasets, and vulnerable data subjects.

#### **5.1.4. Guidelines on processing of personal data through video devices**

During its July plenary meeting, the EDPB also adopted the [Guidelines 3/2019 on processing of personal data through video devices](#).

The Guidelines clarify how the GDPR applies to the processing of personal data in the context of video surveillance, and cover both traditional video devices and smart video devices. For the latter, the Guidelines focus on the rules regarding the processing of special categories of data.

Other areas covered by the Guidelines include the lawfulness of processing, the applicability of the household exemption, and the disclosure of footage to third parties.

The Guidelines were subject to a public consultation, which closed on 9 September 2019. A final version of the document was adopted by the EDPB in early 2020, taking into account input from the consultation.

#### **5.1.5. Guidelines on Data Protection by Design and by Default**

During its fifteenth plenary meeting on 13 November 2019, the EDPB adopted the [Guidelines 4/2019 on Article 25 Data Protection by Design and by Default](#).

The Guidelines focus on the obligation of Data Protection by Design and by Default as set forth in Article 25 GDPR. This requires that controllers implement appropriate technical and organisational measures, as well as the necessary safeguards, to establish data protection principles and to protect the rights and freedoms of data subjects. Controllers must also be able to demonstrate that the implemented measures are effective.

## In 2019, the EDPB adopted Guidelines concerning Codes of Conduct, data processing in the context of online services and through video devices, Data Protection by Design and by Default, and the Right to be Forgotten.

The Guidelines cover elements that controllers must take into account when designing the processing, such as the cost of setting up and maintaining up-to-date technology, in addition to the nature, scope, context, and purpose of the processing itself. The Guidelines also contain practical guidance on how to effectively implement data protection principles, listing key design and default elements as well as illustrating practical cases.

The Guidelines were submitted for public consultation, which remained open until 16 January 2020. A final version of the document will be adopted by the EDPB later in 2020, taking this consultation into account.

#### **5.1.6. Guidelines on the Right to be Forgotten**

During its sixteenth plenary meeting on 2 December 2019, the EDPB adopted the first part of the [Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR](#).

The Guidelines provide an interpretation of Article 17 GDPR, which outlines the “Right to request delisting”. Following the Costeja vs. Google Spain judgment of the Court of Justice of the European Union (CJEU) of 13 May 2014, which established this right, a data subject may request that a search engine provider erase webpage links redirecting to his or her personal data.

The Guidelines seek to establish the grounds and exceptions for delisting requests made to search engine providers.

To gather feedback on the Guidelines, the EDPB launched a public consultation, open until 5 February 2020.

#### **5.1.7. Guidelines adopted following public consultation**

In 2019, the EDPB approved a final version of three Guidelines already adopted in draft form in 2018.

- **Guidelines on Certification and Identifying Certification Criteria:** On 23 January 2019, the EDPB adopted the final version of the core text of [Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the GDPR](#), taking into account the contributions received during a public consultation. The primary aim of these Guidelines is to identify relevant criteria for certification mechanisms, which can be used by organisations to demonstrate compliance with the GDPR.
- On the same day, the **Annex on the Guidelines on Certification and Identifying Certification Criteria** was adopted and submitted for public consultation. The Annex identifies topics that SAs and the EDPB will consider and apply for the approval of certification criteria for a certification mechanism. The entire Guidelines, including a corrigendum and the Annex,

were finalised in June 2019.

- **Guidelines on Accreditation and Certification Bodies:** These Guidelines were adopted on 6 February 2018. The core text was finalised on 4 December 2018. On the same day, Annex 1 was adopted. The entire Guidelines, including Annex 1, were adopted in their final form in June 2019.
- **Guidelines on Territorial Scope:** On 12 November 2019, the EDPB adopted the final version of the [Guidelines 3/2018 on the territorial scope of the GDPR \(Article 3\)](#), following a public consultation. These Guidelines assess whether a particular data processing operation falls within the territorial scope of the GDPR and clarify the application of the Regulation in various situations, for example, when the data controller or processor is established outside the EEA.

#### **5.2. CONSISTENCY OPINIONS**

National SAs from EEA countries must request an Opinion from the EDPB before adopting any decision on subjects specified by the GDPR as having cross-border implications. This applies when a national SA:

- intends to adopt a list of the processing operations subject to the requirement for a Data Protection Impact Assessment (DPIA);
- intends to adopt a draft code of conduct relating to processing activities;
- aims to approve the criteria for accreditation of a certification body;
- aims to adopt standard data protection clauses or contractual clauses;
- aims to approve binding corporate rules.

The competent SA has to take utmost account of the Opinion. In addition, any SA, the Chair of the EDPB or the Commission may request that any matter of general application or which has consequences for more than one Member State be examined by the EDPB with a view to obtaining an Opinion. This can also apply in cases where a competent SA does not comply with obligations for mutual assistance or for joint operations.

The aim of these Opinions is to guarantee the consistent application of the GDPR by national SAs.

#### **5.2.1. Opinions on the draft Data Protection Impact Assessment lists (DPIAs)**

In 2019, the EDPB adopted five Opinions on the draft lists submitted by national SAs on processing operations which require a DPIA, namely those submitted by SAs in [Liechtenstein](#), [Norway](#), [Spain](#), [Iceland](#), and [Cyprus](#).

These lists form an important tool for the consistent application of the GDPR across the EEA. DPIA is a process that helps to identify and mitigate data protection risks that may affect the rights and freedoms of individuals.

While in general the data controller must assess if a DPIA is required before engaging in the processing activity, national SAs must establish and list the kind of processing operations for which a DPIA is required.

These Opinions follow the 26 DPIA-related Opinions adopted by the EDPB in 2018, and will further contribute to establishing common criteria for assessing where DPIAs are required.

In addition, the EDPB also issued three Opinions on the draft lists submitted by SAs in the [Czech Republic](#), [Spain](#) and [France](#) on the processing operations exempt from a DPIA.

Contrary to the “black lists”, the adoption of “white lists” of DPIAs are not mandatory for EEA SAs.

#### **5.2.2. Opinion on transfers of personal data between EEA and non-EEA Financial Supervisory Authorities**

During its seventh plenary meeting on 12 February 2019, the EDPB adopted [Opinion 4/2019 on the draft Administrative Arrangement for the transfer of personal data between European Economic Area \(EEA\) Financial Supervisory Authorities and non-EEA Financial Supervisory Authorities](#).

The [Administrative Arrangement](#) is based on Article 46.3.b GDPR and outlines rules and commitments for transfers

of personal data between EEA Financial Supervisory Authorities, including the European Securities and Markets Authority (ESMA), and their non-EEA counterparts.

Following the Opinion, this arrangement will be submitted to the competent SAs for authorisation at national level. The EDPB recommends that the SAs monitor the arrangement and its practical application to ensure that data subject rights and appropriate means of redress and supervision are effective and enforceable in practice.

#### **5.2.3. Opinion on the interplay between the ePrivacy Directive and the GDPR**

During its eighth plenary meeting on 13 and 14 March 2019, the EDPB adopted [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](#).

The Opinion seeks to clarify whether the processing of personal data falls under the scope of both the GDPR and the ePrivacy Directive, and whether this limits the competences, tasks and powers of data protection authorities under the GDPR.

The EDPB is of the opinion that SAs are competent to enforce the GDPR. The fact that a subset of the processing falls within the scope of the ePrivacy Directive does not limit the competence of SAs under the GDPR.

Indeed, an infringement of the GDPR may at the same time constitute an infringement of national ePrivacy rules. SAs may take this into consideration when applying the GDPR (e.g. when assessing compliance with the lawfulness or fairness principles).

#### **5.2.4. Opinion on the competence of a Supervisory Authority in case of a change in circumstances relating to the main or single establishment**

During its twelfth plenary meeting on 9 and 10 July 2019, the EDPB adopted [Opinion 8/2019 on the competence of a Supervisory Authority in case of a change in circumstances relating to the main or single establishment](#).

The scenario outlined in the Opinion may occur when the main establishment is relocated within the EEA, or is moved to the EEA from a third country, or when there no longer is a main or single establishment in the EEA. In such circumstances, the EDPB is of the opinion that the competence of the Lead Supervisory Authority (LSA) can switch to another SA.

In this case, the cooperation procedure set forth under Article 60 GDPR will continue to apply and the new LSA will be obligated to cooperate with the former LSA, as well as the other concerned SAs (CSAs), to reach a consensus. The switch can take place as long as no final decision has been reached by the competent SA.

#### **5.2.5. Opinions on Accreditation Criteria for monitoring bodies of Codes of Conduct**

During its July plenary meeting, the EDPB also adopted [Opinion 9/2019 on the Austrian data protection supervisory authority draft accreditation requirements for a code of conduct monitoring body pursuant to Article 41 GDPR](#). The EDPB agreed that all codes covering non-public authorities and bodies are required to have accredited monitoring bodies in accordance with the GDPR.

In addition, during its sixteenth plenary meeting on 2 and 3 December 2019, the EDPB adopted [Opinion 17/2019 on the UK data protection supervisory authority draft accreditation requirements for a code of conduct monitoring body pursuant to Article 41 GDPR](#). In this Opinion, the EDPB proposed some changes to the draft accreditation requirements in order to ensure consistent application of the accreditation of monitoring bodies.

#### **5.2.6. Opinion on Standard Contractual Clauses for processors by Danish SA**

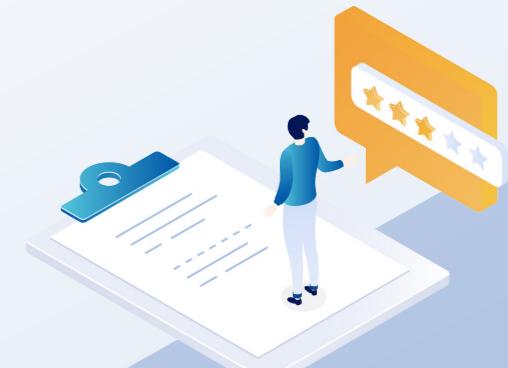
In July, the EDPB adopted [Opinion 14/2019 on the draft Standard Contractual Clauses \(SCCs\) submitted by the DK SA \(Article 28.8 GDPR\)](#). As the first Opinion on this topic, it aims to ensure the consistent application of Article 28.8 GDPR for contracts between controller and processor.

Standard Contractual Clauses (SCCs) aim to help organisations meet the requirements of Article 28.3 and 28.4 GDPR, given that the contract between controller and processor cannot simply restate the provisions of the GDPR but should further specify them, e.g. with regard to the assistance provided by the processor to the controller.

**National SAs from EEA countries must request an Opinion from the EDPB before adopting any decision on subjects specified by the GDPR as having cross-border implications.**

The EDPB made several recommendations which were taken into account by the Danish SA, which subsequently updated the draft SCCs.

The possibility of using SCCs adopted by an SA does not prevent the parties from adding other clauses or additional safeguards, provided that they do not, directly or indirectly contradict the adopted clauses or prejudice data subjects' fundamental rights or freedoms.





Nevertheless, the clauses are an instrument to be used ‘as is’, i.e. the parties who enter into a contract with a modified version of the clauses are not considered to have used the adopted SCCs.

#### **5.2.7. Opinions on Binding Corporate Rules**

During its fourteenth plenary meeting on 8 and 9 October 2019, the EDPB adopted [Opinion 15/2019 on the draft decision of the competent Supervisory Authority of the United Kingdom regarding the Binding Corporate Rules \(BCRs\) of Equinix Inc](#), following a request by the UK Information Commissioner’s Office (ICO).

The EDPB is of the opinion that the Equinix BCRs contain all elements required under Article 47 GDPR and WP 256 rev01, and contain the appropriate safeguards.

In case of Brexit, the company committed to initiate a new process of approval with an alternative SA as new Lead BCR SA without undue delay and, in the event, within one calendar month.

During its November plenary meeting, the EDPB adopted [Opinion 16/2019 on the draft decision of the Belgian Supervisory Authority regarding the Binding Corporate Rules of ExxonMobil Corporation](#).

The EDPB is of the opinion that the draft controller BCRs provide sufficient safeguards in line with Article 46.2.b GDPR and comply with Article 47 GDPR.

#### **5.3. LEGISLATIVE CONSULTATION**

The EDPB advises the European Commission on any issue related to the protection of personal data, on the format and procedures for information exchange between companies and SAs under Binding Corporate Rules (BCRs), and on certification requirements. The EDPB also advises the European Commission when assessing the adequacy of the level of data protection in third countries or international organisations.

In 2019, the EDPB issued an [Opinion on the interplay between the Clinical Trials Regulation \(CTR\) and the GDPR](#), requested by the European Commission’s Directorate-General for Health and Food Safety (DG SANTE).

The EDPB is also subject to Article 42 of [Regulation 2018/1725](#) on legislative consultation. This allows the EDPS and the EDPB to coordinate their work with a view to issuing a Joint Opinion.

In 2019, the EDPB and the EDPS adopted a [Joint Opinion concerning the data protection aspects of the eHealth Digital Service Infrastructure](#). This Opinion was also issued following DG SANTE’s request.

The EDPB also adopted, on its own initiative, [a statement on the draft ePrivacy Regulation and issued a contribution on the data protection aspects of the Budapest Convention on Cybercrime](#).

#### **5.3.1. EU-U.S. Privacy Shield**

Representatives of the EDPB participated in joint reviews of the EU-U.S. Privacy Shield adequacy decision, conducted by the European Commission to assess its robustness and practical implementation. The EDPB issued reports on the Second and Third Annual Review of the EU-U.S. Privacy Shield.

During its January plenary meeting, the EDPB adopted its report on the [Second Annual Joint Review of the EU-U.S. Privacy Shield](#), which was conducted by the European Commission in October 2018 with the support of the EDPB’s representatives.

The EDPB welcomed efforts made by the United States authorities and the European Commission to implement the EU-U.S. Privacy Shield, such as adapting the initial certification process, starting ex-officio oversight and expanded enforcement. These actions also included enhanced transparency, following the decision to publish a

number of important documents, in part via declassification by the United States Foreign Intelligence Surveillance Court.

The EDPB also welcomed the appointment of a new Chair and three new members of the Privacy and Civil Liberties Oversight Board (PCLOB), and a permanent Ombudsperson.

However, the EDPB had a number of significant concerns – already expressed by the EDPB’s predecessor, the Article 29 Working Party (WP29) – about the lack of concrete assurances aimed at excluding indiscriminate collection and access of personal data for national security purposes.

In addition, the EDPB did not consider the Ombudsperson to have been vested with sufficient powers to remedy non-compliance. The EDPB also pointed out that checks regarding compliance with the substance of the EU-U.S. Privacy Shield’s principles were not sufficiently strong.

The EDPB had some additional concerns about the checks needed to comply with the onward transfer requirements, the scope of the meaning of HR Data, and the recertification process, as well as several issues still pending after the first joint review.

During its November plenary meeting, the EDPB adopted its [Third Annual Joint Review](#) report on the EU-U.S. Privacy Shield. In its report, the Board welcomed the appointments of the last missing members of the PCLOB and noted that several issues previously raised remained unsolved. More generally, the EDPB found that the Review Team members would benefit from broader access to non-public information concerning commercial aspects and ongoing investigations.

Regarding the collection of data by public authorities, the EDPB encourages the PCLOB to issue and publish further reports in order to provide an independent assessment of surveillance programmes conducted outside U.S. territory, when data is transferred from the EU to the U.S. The EDPB reiterated that its security-cleared experts remain ready to review further documents and discuss additional classified elements.

While the EDPB welcomed the new elements provided during the 2019 review process, it still could not conclude

that the Ombudsperson is vested with sufficient powers to access information and remedy non-compliance.

#### **5.3.2. Opinion on clinical trials Q&A**

Under Article 70 GDPR, the European Commission can submit a request for consultation to the EDPB. In 2018, the Commission’s DG SANTE requested a consultation on a document on “Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR)”.

The EDPB subsequently adopted [Opinion 3/2019](#) during its January plenary meeting. The Opinion addressed in particular the adequate legal bases of personal data processing in the context of clinical trials and the secondary uses of clinical trial data for scientific purposes.

#### **5.3.3. Statement on the future ePrivacy Regulation**

During its eighth plenary meeting in March 2019, the EDPB adopted [Statement 3/2019 on an ePrivacy regulation](#).

The EDPB called upon EU legislators to intensify efforts towards the adoption of the ePrivacy Regulation, which is essential to complete the EU’s data protection framework and the confidentiality of electronic communications.

The future ePrivacy Regulation should under no circumstance lower the level of protection offered by the current ePrivacy Directive and should complement the GDPR by providing additional guarantees for all types of electronic communications.

#### **5.3.4. Additional protocol to the Budapest Convention on Cybercrime**

In November 2019, the EDPB adopted a [contribution to the draft second additional protocol to the Council of Europe Convention on Cybercrime \(Budapest Convention\)](#), to be considered within the framework of consultations held by the Council of Europe Cybercrime Committee (T-CY).

The EDPB highlighted that the protection of personal data and legal certainty must be guaranteed, thus contributing to establishing sustainable arrangements for the sharing of personal data with third countries for law enforcement

purposes, which are fully compatible with the EU Treaties and the Charter of Fundamental Rights.

#### **5.3.5. EDPB-EDPS Joint Opinion on the eHealth Digital Service Infrastructure**

During its July 2019 plenary meeting, the EDPB and the EDPS adopted [Joint Opinion 1/2019 on the processing of patients' data and the role of the European Commission within the eHealth Digital Service Infrastructure \(eHDSI\)](#).

This was the first Joint Opinion by the EDPB and the EDPS. It was adopted in response to a request from the European Commission under Article 42.2 of Regulation 2018/1725 on data protection for EU institutions and bodies.

The eHealth Network is a voluntary network of authorities responsible for eHealth, as designated by Member States. One of its main objectives is to enhance interoperability between national digital health systems, by exchanging patient data contained in ePrescriptions, Patient Summaries and electronic health records. In this framework, the eHealth Network and the Commission have developed an IT tool, the eHealth Digital Service Infrastructure (eHDSI).

In their Opinion, the EDPB and EDPS considered that, in this specific situation and for the concrete processing of patients' data within the eHDSI, there was no reason to dissent from the European Commission's assessment of its role as a processor within the eHDSI. Furthermore, the Joint Opinion stressed the need to ensure that all processing duties of the Commission in this operation were clearly set out in the relevant Implementing Act, as specified in the applicable data protection legislation.

#### **5.4. OTHER DOCUMENTS**

##### **5.4.1. Information note on data transfers under the GDPR in the event of a no-deal Brexit**

During its February 2019 plenary, the EDPB adopted an information note on [data transfers under the GDPR in the event of a no-deal Brexit](#), addressed to commercial entities and public authorities.

With regards to the transfer of personal data **from the EEA**

**to the UK**, the EDPB recommended basing the process on one of the following instruments:

- Standard or ad hoc Data Protection Clauses;
- Binding Corporate Rules;
- Codes of Conduct and Certification Mechanisms;
- Specific instruments available to public authorities.

In the absence of Standard Data Protection Clauses or other alternative appropriate safeguards, derogations can be used under certain conditions, as outlined by Article 49 GDPR.

##### **5.4.2. Information note on Binding Corporate Rules for companies which have the UK Information Commissioner's Office as BCR Lead Supervisory Authority**

In February 2019, the EDPB also issued an information note to companies having the UK Information Commissioner's Office (ICO) as their BCR LSA in the event of a no-deal Brexit.

##### **5.4.3. Statement on the US Foreign Account Tax Compliance Act**

On 25 February 2019, the EDPB adopted [Statement 01/2019 on the US Foreign Account Tax Compliance Act \(FATCA\)](#), following the European Parliament's resolution on the adverse effects of the FATCA on EU citizens.

European SAs have long been aware of the data protection issues raised by the automatic exchange of personal data for tax purposes. In its statement, the EDPB referred to previous work on the FATCA by its predecessor, the Article 29 Working Party (WP29).

The EDPB also acknowledged the Parliament's call to review existing data protection safeguards authorising the transfer of personal data to the United States' Internal Revenue Service (IRS) for the purposes of the FATCA. In this regard, the EDPB has already initiated work on Guidelines on the elaboration of transfer tools based on Articles 46.2.a and 46.3.b GDPR.

These Guidelines will include information on minimum guarantees to be included in legally binding and enforceable instruments concluded between public authorities and bodies, as well as data protection provisions to be included

in administrative arrangements between public authorities or bodies.

It should be noted that legally binding instruments do not require specific authorisation from an SA, whereas any provisions to be included in administrative arrangements are subject to such authorisation.

This set of Guidelines, to be adopted in 2020, will also be a useful tool for evaluating the compliance of intergovernmental agreements signed between Member States and the United States government on FATCA with the GDPR.

##### **5.4.4. Statement on the use of personal data in political campaigns**

During its March 2019 plenary meeting, the EDPB adopted [Statement 2/2019 on the use of personal data in the course of political campaigns](#), in light of the 2019 European Parliament elections and other elections taking place across the EU and beyond.

Data processing techniques for political purposes can pose serious risks to privacy and data protection rights, as well as to the integrity of the democratic process. In its statement, the EDPB highlighted a number of key points to be taken into consideration when political parties process personal data during their electoral activities.

1. Under the GDPR, personal data revealing political opinions is a special category of data and its processing is heavily limited, if not entirely prohibited.
2. Personal data made public, for example on social media, is still subject to EU data protection law.
3. Even where data processing is lawful, organisations must respect their duties of fairness and transparency to individuals whose data has been collected. Political parties and candidates must stand ready to demonstrate how they have complied with data protection principles.
4. Automated decision-making, including profiling, is only lawful with the valid explicit consent of the data subject.
5. In case of targeting, adequate information should be provided to voters explaining why they are receiving

a particular message, who is responsible for it, and how they can exercise their rights as data subjects. In addition, certain Member States require transparency in matters of paid political advertisements.

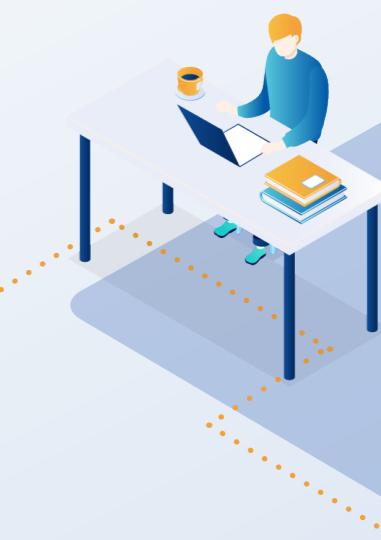
The EDPB's statement reiterated the importance of compliance with data protection rules to protect democracy, preserve citizens' trust and confidence, and safeguard the integrity of elections. The EDPB encourages maximum cooperation among SAs in monitoring and enforcing these rules.

#### **5.4.5. LIBE Report on the implementation of the GDPR**

On 26 February 2019, the [EDPB LIBE report on the implementation of GDPR](#) was issued following a request made by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs Committee (LIBE).

This document provides an overview of the implementation and enforcement of the GDPR covering both the cooperation mechanism and the consistency findings.

Nine months after the GDPR's entry into application, the EDPB concluded that the GDPR cooperation and consistency mechanism works quite well in practice. National SAs make daily efforts to facilitate this cooperation, via written and oral communication.



However, these cooperation duties do entail additional workload and time resources, which in turn can have an impact on SAs' budgets. The handling of cross-border cases in particular takes a considerable amount of time, given the need for thorough investigations and compliance with national procedural rules. The EDPB noted that national SAs must tackle challenges regarding the harmonized enforcement of the GDPR.

Finally, while the EDPB reported six final One-Stop-Shop (OSS) cases, it could not provide testimony about the effectiveness of the consistency mechanism for these, since no dispute resolution was necessary during the reporting period.

#### **5.4.6. EDPB pleading before the CJEU in Case C-311/18 (Facebook Ireland and Schrems)**

On 9 July 2019, the EDPB Chair appeared before the Court of Justice of the European Union (CJEU), which requested an oral [pleading on Case C-311/18 \(Facebook Ireland and Schrems\)](#).

The case arose from a preliminary reference made by the Irish High Court to the CJEU, following a legal challenge brought by Austrian privacy activist Max Schrems in relation to Facebook's use of Standard Contractual Clauses (SCCs) to transfer data from Facebook Ireland to servers located in the United States. Mr. Schrems argued that Facebook Inc.'s obligation to make the personal data of its users available to the United States authorities in charge of surveillance programmes threatened the exercise of the rights guaranteed in Article 7, 8 and 47 of the Charter, and that no remedies were put in place. In this context, the CJEU invited the EDPB to participate in the oral hearing that took place on 9 July 2019.

In its pleading, the EDPB answered several questions asked by the CJEU. The EDPB underlined the difference between SCCs and adequacy decisions and stated that, with regard to the SCCs, the European Commission is not obliged to examine the continuity of the protection afforded by EU law. In this regard, the EDPB considered that verifying the compliance of transfers with the EU data protection law when considering whether to enter into the SCCs should be primarily the responsibility of the exporter and the importer.

This should be further assessed by the competent SA, which may suspend transfers if it finds that exporter and importer did not comply with their obligations under the SCCs.

The EDPB's view was that the continuity of data protection afforded under EU laws also needs to be ensured during data transit to a third country, no matter which transfer tool is used. This includes data outside or on its way to the EU's physical borders.

With regard to questions on adequacy decisions, the EDPB stated that all domestic rules are relevant for the assessment of adequacy and that data subjects should be able to enforce their rights before the third country's courts. In this regard, even though the establishment of the Ombudsperson mechanism under the Privacy Shield framework is welcomed, the EDPB stressed that it cannot conclude that the Ombudsperson constitutes an effective remedy before a tribunal in the meaning of Article 47 of the Charter of Fundamental Rights.

Finally, the EDPB stressed the importance of the role of the SAs in upholding and spreading EU standards on the fundamental right to data protection.

At the time of this report going to press, the CJEU had not yet issued a final ruling on the case.

#### **5.5. PLENARY MEETINGS AND SUBGROUPS**

Between 1 January and 31 December 2019, the EDPB held 11 plenary meetings. The agendas of the plenary sessions are published on the EDPB website. During these meetings, the EDPB adopted Guidelines, Opinions, and other documents such as statements or informative notes to advise the European Commission, national Supervisory Authorities, and other stakeholders on GDPR matters, as outlined earlier in this chapter.

In addition, there were 90 expert subgroup meetings. The different expert subgroups focus on specific areas of data protection and assist the EDPB in performing its tasks. The list of the expert subgroups and their respective mandates are available in Section 9.



### **5.6. STAKEHOLDER CONSULTATIONS AND TRANSPARENCY**

#### **5.6.1. Stakeholder events on future guidance**

The EDPB organises stakeholder events to gather input and views on issues in the interest of developing future guidance. In 2019, the EDPB organised three such events focusing on the revised Payments Services Directive (PSD2), on the concepts and responsibilities of controllers and processors, and on data subject rights.

##### **5.6.1.1. Interplay of PSD2 and GDPR**

On 27 February 2019, the EDPB's Financial Matters Expert Subgroup (FMES) organised a workshop on the revised Payments Services Directive (PSD2), in order to collect stakeholders' views and inform future Guidelines.

**The EDPB organises stakeholder events to gather input and views on issues in the interest of developing future guidance.**

Of the event's 39 participants, 16 were external stakeholders. Representatives from banking federations, payment institutions

federations, consumer protection associations, academia, and the European Commission's Directorate-General for Financial Stability, Financial Services and Capital Markets Union (DG FISMA) presented at the workshop. Other participants included collection associations, credit information suppliers, banks, and financial market associations.

The discussions highlighted the key areas already identified by the FMES where guidance is required, as well as providing concrete examples. The feedback will be used as basis for developing Guidelines on PSD2.

##### **5.6.1.2. Concepts of controller and processor**

On 25 March 2019, the EDPB organised a full-day stakeholder event to gather the views of EU sector organisations and NGOs in the context of the EDPB's recast of the Article 29 Working Party's [Opinion 1/2010 on the concepts of controller and processor](#). Around 80 participants, including EDPB representatives, attended the event, which received positive feedback overall.

To facilitate greater engagement, core discussions took place in three smaller breakout sessions with rotating rapporteurs and moderators. Each group addressed the following topics:

- **The concepts of controller and processor:** issues raised related to the relationship between controllers and processors, the main criteria for identifying the controller, clarification of other concepts such as

- recipient and third party, and the consistent application of the Guidelines. Additionally, stakeholders suggested including as many practical examples as possible.
- The specific obligations of processors and the contracts between controllers and processors:** stakeholders highlighted the need to revise the current guidance to reflect changes in the legal framework and the business environment, and voiced concern over the difficulty to implement certain new duties for processors, especially SMEs. Stakeholders also identified a need for guidance on the controller's audit rights, the obligation for the processor to inform the controller in case of an infringement, and duties regarding sub-processors.
  - Joint controllership:** stakeholders once more stressed the changed business context for data sharing and highlighted difficulties when incorporating practical duties in contracts. They suggested that guidance should further clarify the criteria to be taken into account when determining whether the relationship qualifies as joint controllership.

The feedback provided by stakeholders and especially the need for practical examples will be considered when drafting the guidelines.

#### 5.6.1.3. Data subject rights

On 4 November 2019, the EDPB organised a full-day stakeholder event on the topic of data subject rights. Attendees included representatives from individual companies, sector organisations, NGOs, law firms, and academia.

Developing guidance on data subject rights is one of the EDPB's 2020 priorities. During the event, around 160 participants, including EDPB representatives, had the opportunity to share their experiences on this topic and raise issues.

The workshop followed a similar format as the March 2019 event, which proved to be engaging for stakeholders. Discussions were spread across three smaller breakout sessions with rotating rapporteurs and moderators, each addressing the following topics:

- Right of access:** issues raised related to the type and format of information requested, formal requirements such as identity verification and dedicated channels,

- and clarifications on third-party access requests.
- Right to rectification and right to erasure:** stakeholders shared concerns on differences and interplays between rights, technical means and proof of erasure, and requests involving joint controllers or controllers outside the EEA.
  - Right to restrict processing and right to object:** stakeholders asked for concrete examples, as well as guidance on the practical implementation of restriction and issues of legitimate interest, especially related to direct marketing.

The EDPB will take into account input provided during the workshop, including the practical examples shared by the stakeholders, the guidance requested and the questions raised. In 2020, the relevant expert subgroup will further discuss the topics and work on Guidelines.

#### 5.6.2. Public consultations on draft guidance

Following the preliminary adoption of Guidelines, the EDPB organises public consultations to give stakeholders and citizens the opportunity to provide additional input. This input is then taken into account by the EDPB members in charge of drafting. Next, the Guidelines are adopted in their final version.

To further enhance transparency, the EDPB adapted its website to enable the publication of stakeholders' contributions to public consultations.

In 2019, the EDPB launched five such consultations:

- In February, the EDPB opened two public consultations, on [Guidelines on Codes of Conduct \(1/2019\)](#) and on the [Annex to the Guidelines on Certification \(1/2018\)](#), for which it received 44 and 8 contributions respectively. The final versions of the Guidelines and of the Annex, including further points of clarification, were adopted in June.
- In April, the EDPB opened a public consultation on [Guidelines on the processing of personal data in the context of online services \(2/2019\)](#), receiving 45 contributions.
- In July, the EDPB opened a public consultation on [Guidelines on video surveillance \(3/2019\)](#), receiving 94 contributions.
- In November, the EDPB opened a public consultation on [Guidelines on Data Protection by Design and by Default](#)

(4/2019). This consultation was still open at the end of 2019.

- In December, the EDPB opened a public consultation on [Guidelines on the Right to be Forgotten in the search engine cases \(5/2019\)](#). This consultation was still open at the end of 2019.

#### 5.6.3. Stakeholder survey on adopted guidance

For the second year in a row, the EDPB conducted a survey as part of the annual review of the Board's activities under Article 71.2 GDPR. Questions focused on the content and adoption process of the EDPB's Guidelines, with a view to understanding to what extent stakeholders find them helpful and practical to interpret GDPR's provisions.

##### 5.6.3.1. Participants

53 entities including organisations and individual companies, representing different countries, sectors and business sizes participated in the survey. The majority of respondents were based in Europe (50 organisations), while the remaining three were based in North America.

The financial, banking and insurance sector was the most represented, with 17 contributors, followed by wholesale and retail trade (nine respondents), information technologies (six respondents), human health and social work activities (six respondents), and human and fundamental rights (three respondents).

More than 60 percent of respondents were representing small entities, with less than 250 employees.

The results showed that participants had consulted, on average, four Guidelines.

##### 5.6.3.2. Findings

In line with the results of the 2018 survey, 64 percent of stakeholders participating in the survey found the Guidelines to be useful and 46 percent considered them to be sufficiently pragmatic and operational for their needs. One of the suggestions was to avoid long pages of guidelines and to include checklists to better guide the companies.

In addition, 62 percent of those who responded to the survey found the Guidelines easy to read. There was a

marked increase of respondents who found the guidelines easily accessible on the EDPB's website: nearly 80 percent, up from 64 percent in 2018.

On the first section of the survey, dedicated to the Guidelines' content, the majority of respondents welcomed the pan-European applicability of the Guidelines, judging that this prevents national fragmentation. Half of the respondents judged the Guidelines to provide sufficient examples in their respective area of regulation, and one of the respondents expressed appreciation for the fact that the EDPB guidelines include many real-life examples.

**Stakeholders encouraged further interpretative work but noted that the Guidelines are a useful tool in supporting the application of the GDPR.**

Further interpretative work was encouraged to clarify, for example, the relationship between controller and processor and the legal basis of legitimate interest. The EDPB welcomes this timely feedback as it schedules an update of the dedicated Article 29 Working Party Guidelines, to be carried out during 2020, in line with the 2019-2020 EDPB Work programme.



Compliance with the GDPR for SMEs remains a challenge, but stakeholders noted that the EDPB's Guidelines are a useful tool in supporting its application.

40 percent of stakeholders found the consultative process appropriate to satisfying. They welcomed the EDPB's openness to public consultations and the opportunities given to express views on the Board's work. Part of the respondents appreciated the clarity and accessibility of the EDPB's workshops, but encouraged further improvements in transparency.

#### **5.6.3.3. Conclusions**

The EDPB highly appreciated the stakeholders' participation and was pleased to see that respondents acknowledged the Guidelines' usefulness. Feedback on the Guidelines' operational value and alignment with other EU laws was equally appreciated, as it gave precious insights into stakeholder needs, and will inform the Board's work moving forward.

The EDPB also welcomed stakeholders' value of transparency and interest in participating in the adoption process. In 2020, the EDPB is committed to continuing its cooperation and outreach to inform the development and effectiveness of future guidance.

#### **5.6.4. Transparency and access to documents**

Transparency is a core principle of the EDPB and in 2020, the EDPB will continue to implement measures designed to increase the transparency of its work. As an EU body, the EDPB is subject to Article 15 of the [Treaty of the Functioning of the European Union and Regulation 1049/2001](#) on public access to documents. Article 76.2 GDPR and Article 32 of the EDPB's Rules of Procedure (RoP) reinforce this requirement.

Upholding the principle of transparency means that any citizen of the European Union and any natural or legal person residing or having its registered office in a Member State has the right to access EDPB documents. This right applies to all documents held by the EDPB, concerning any matter relating to its responsibilities.

In exceptional cases, the EDPB can refuse to disclose a document, or part of it. The reasons for refusal and other procedural rules are outlined in the [EU Public Access Regulation](#).

In 2019, the number of public access requests registered for documents held by the EDPB was 39.

#### **5.7. EXTERNAL REPRESENTATION OF THE BOARD**

Public awareness and cooperation are vital to upholding data protection rights in the EEA and beyond, which is why the EDPB values stakeholder and citizen engagement.

The EDPB Secretariat supports the Chair and the Deputy Chairs in engagements with other EU institutions or bodies and when they represent the EDPB at conferences and multi-stakeholder platforms.

Staff members from the EDPB Secretariat also take part in several events to present the activities of the EDPB.

#### **5.7.1. Participation of Chair and Deputy Chair in conferences and speaking engagements**

##### **5.7.1.1. Chair of the EDPB**

In 2019, EDPB Chair Andrea Jelinek had 34 speaking engagements, including keynote speeches, presentations and panel debates in a range of institutes, think tanks and forums. She also met with EU Commissioners and travelled to meet with data protection officials from countries outside the EEA.

During the G20 meeting in Tokyo, Japan, the Chair took part in a side event entitled "**DPA's role in Global Data Flows**", held on 3 July 2019 and organised by the Japanese Data Protection Authority.

In her opening remarks, the Chair explained the role of the EDPB, its activities so far and the importance of international convergence. She also talked about the EU-Japan adequacy decision, stressing its importance as a model for successful international cooperation.

On 9 July, the Chair was invited to a **hearing at the Court of Justice of the European Union** (CJEU) in Luxembourg, concerning Case C-311/18 (Facebook Ireland and Schrems).

The Chair of the EDPB also met twice with the **European Parliament's Committee on Civil Liberties, Justice and Home Affairs Committee** (LIBE Committee), in February and in December. These meetings provided the opportunity

to present the EDPB's work and to give an overview of GDPR's implementation.

In 2019, the EDPB became Observer of the **International Conference of Data Protection and Privacy Commissioners** (ICDPPC, now the Global Privacy Assembly – GPA). During the October annual meeting held in Tirana, Albania, the Chair presented the EDPB's work and outlined the GDPR's main provisions, including the cooperation and consistency mechanism.

The Chair of the EDPB also participated in other high-level forums on data protection, such as the **Europe Data Protection Congress** and the **Global Summit of the International Association of Privacy Professionals** (IAPP).

##### **5.7.1.2. Deputy Chair of the EDPB**

EDPB Deputy Chair Ventsislav Karadjov took part in six speaking engagements during 2019, mainly in the EU but also in the United States, on the occasion of the third annual review of the EU-U.S. Privacy Shield.

As well as taking part in events organised by the European Commission and the European Union Agency for Cybersecurity (ENISA), the Deputy Chair attended high-level platforms such as the Mobile World Congress (MWC) ministerial meeting, where he spoke about GDPR, data privacy and blockchain.

#### **5.7.2. Participation of the EDPB Members in conferences and speaking engagements**

In 2019, EDPB Members represented the EDPB in a number of events. Some of these were organised by trade, consumer, or professional associations dealing with aspects of data protection and the implementation of the GDPR, while other invitations came from academia and think tanks.

Several engagements were organised on the initiative of EU institutions and bodies, such as the European Central Bank, the European Ombudsman, and the European Parliament's LIBE Committee.

EDPB representatives also participated in high-level forums on data protection, such as the ICDPPC and the IAPP Europe Data Protection Congress and Global Summit.

#### **5.7.3. Participation of the EDPB Secretariat Staff in conferences and speaking engagements**

In 2019, EDPB Secretariat staff members participated in 35 conferences or other engagements with an average of three per month. They were usually invited to deliver speeches or presentations or to join panel discussions.

#### **5.7.4. Election of representative and substitute to the Stakeholders Cybersecurity Certification Group**

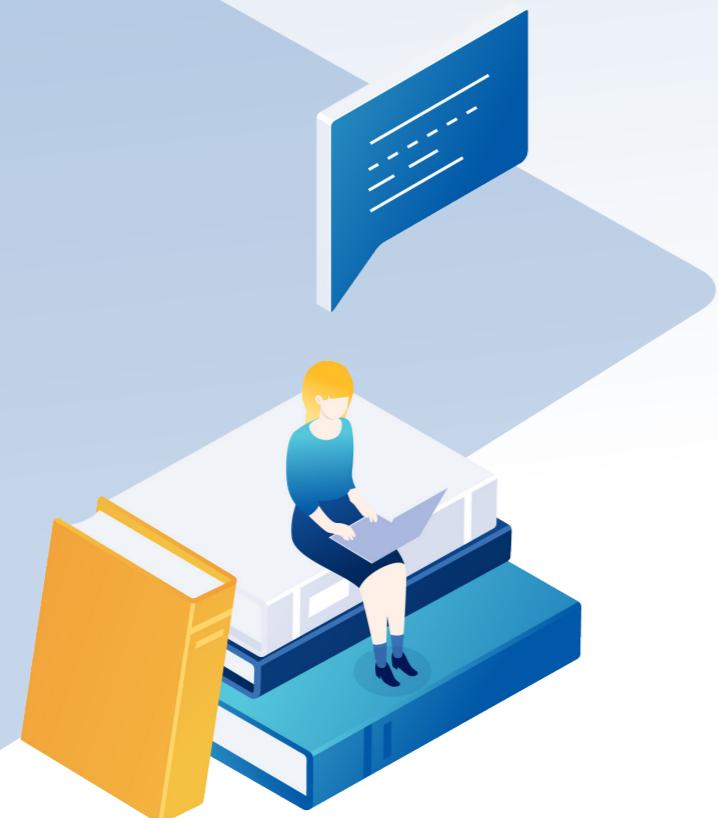
During its December 2019 plenary meeting, the EDPB confirmed the appointments of the representative and substitute to the Stakeholders Cybersecurity Certification Group.

The Group was established by the [Cybersecurity Act](#), which entered into force on 27 June 2019. Among its provisions, the Act seeks to establish an EU-wide cybersecurity certification framework. The Group's goal is to provide appropriate governance at the EU level and to support ENISA and the European Commission in facilitating consultation with relevant stakeholders.

The Cybersecurity Act identifies EU SAs as such stakeholders. For this reason, the European Commission's Directorate-General for Communications Networks, Content and Technology (DG CNECT) sent a letter to the EDPB on 1 October 2019, requesting that a representative and a substitute for the Group be appointed.

The Compliance, eGovernment and Health Expert Subgroup (CEH ESG), which has a mandate to deal with certification and accreditation topics, evaluated candidates who volunteered to act as EDPB representatives to the Group. During its meeting of 15 November 2019, the CEH ESG nominated Mr. Desmond de Haan, from the Netherlands, as representative and Ms. Georgia Panagopoulou, from Greece, as substitute. They were subsequently approved and appointed by the EDPB.

# 6



## Supervisory Authority activities in 2019

Under the GDPR, Supervisory Authorities (SAs) have a duty to cooperate in order to ensure consistent application of the Regulation. In cases that have a cross-border component, the SAs of the European Economic Area (EEA), i.e. the 28 EU Member States (27 as of 31 January 2020) plus Iceland, Norway and Liechtenstein, have a range of tools at their disposal to facilitate harmonisation. These are:

- mutual assistance;
- joint operation;
- the One-Stop-Shop cooperation mechanism.

### 6.1. CROSS-BORDER COOPERATION

#### 6.1.1. Preliminary procedure to identify the Lead and Concerned Supervisory Authorities

Before starting a One-Stop-Shop procedure for a cross-border case, it is necessary to identify the Supervisory Authority that will lead the investigation (LSA) and the other Concerned Supervisory Authorities (CSAs). The LSA will lead the investigation and draft the decision, while the CSAs will have the opportunity to raise objections.

The LSA is identified as the authority of the EEA country where the data controller or processor under investigation has its main establishment. For example, the place of central administration is one of the criteria used to identify a controller or processor's main establishment.



Further information on this subject is available in Article 1.2 of the [Article 29 Working Party Guidelines for identifying a controller or processor's lead Supervisory Authority](#), endorsed by the EDPB at its first plenary meeting on 25 May 2018.

The EDPB created workflows in the Internal Market Information System (IMI) to enable SAs to identify their respective roles. This IT platform is used to support cooperation and consistency procedures under the GDPR. The main purpose of this procedure is to define roles at an early stage.

In case of conflicting views regarding which authority should act as LSA, the EDPB will act as a dispute resolution body and issue a binding decision.

Since 25 May 2018, 807 procedures were initiated to identify the LSA and the CSA in cross-border cases. No disputes on the selection of the LSA occurred.

#### 6.1.2. Database regarding cases with a cross-border component

A case with a cross-border component may occur in several situations: when the controller or the processor has an establishment in more than one Member State; when the data processing activity substantially affects individuals in more than one Member State; or when SAs are simply exchanging information, i.e. providing each other with mutual assistance.

Such cases are registered in a central database via the IMI system, from which the aforementioned procedures can be initiated.

Since the entry into application of the GDPR, there were 807 cross-border cooperation procedures in the IMI system, out of which 585 cases were started in 2019. Of these cross-border cooperation procedures, 425 resulted from a complaint, while the others originated from other sources, such as investigations, legal obligations or media reports.

#### 6.1.3. One-Stop-Shop Mechanism

The OSS mechanism demands cooperation between the LSA and the CSAs. The LSA leads the investigation and plays a key role in the process of reaching consensus between the CSAs, in addition to working to reach a coordinated decision with regard to the data controller or processor.

The LSA must first investigate the case while taking into account national procedural rules, ensuring that the affected individuals are able to exercise their right to be heard, for example. During this phase, the LSA can gather information from another SA via mutual assistance or by conducting a joint investigation.

The IMI system also gives the LSA the opportunity to informally communicate with all CSAs to collect relevant information.

Once the LSA has completed its investigation, it prepares a draft decision, which it then communicates to the CSAs. They have the right to object. This either leads to a revised draft decision or, if no consensus can be found, triggers the EDPB's dispute resolution mechanism.

In such cases, the EDPB will act as a dispute resolution body and issue a binding decision. The LSA must adopt its final decision on the basis of the EDPB's decision.

If the CSAs do not object to either the initial draft or the revised decision, they are deemed to agree with the draft decision.

The IMI system offers different procedures that can be followed when handling OSS cases:

- Informal consultation procedures;
- Draft decisions or revised decisions submitted by the LSA to the CSAs;
- Final OSS decisions submitted to the CSAs and to the EDPB.

By the end of 2019, 142 OSS procedures were initiated by SAs, 79 of which resulted in a final decision.



#### 6.1.4. Mutual assistance

The mutual assistance procedure allows SAs to ask for information from other SAs or to request other measures for effective cooperation, such as prior authorisations or investigations.

Mutual assistance can be used for cross-border cases subject to the OSS procedure, either as part of the preliminary phase, to gather the necessary information before drafting a decision or for national cases with a cross-border component.

The IMI system enables the use of either informal mutual assistance without any legal deadline or the use of formal mutual assistance. In the latter case, according to the GDPR, the SA from which information has been requested has a legal deadline of one month to reply.

Since 25 May 2018, 2,542 mutual assistance procedures were triggered. Of these procedures, the overwhelming majority (2,427) were informal consultation procedures, while 115 were formal requests.

## GDPR CASE

### Identification of LSA and CSA - Article 56

Preliminary procedures

### Creation of entry in Case register for the Case

#### Cooperation Procedures

One-Stop-Shop  
Article 60

Mutual Assistance  
Article 61

Voluntary Mutual Assistance  
Article 61

Joint Operations  
Article 62

Local Case Requests  
Article 56

#### Consistency Procedures

Opinion by the EDPB  
Article 64

Dispute Resolution by the EDPB  
Article 65

Urgent Opinion/Decision by the EDPB  
Article 66

#### 6.1.5. Joint operations

The GDPR allows SAs to carry out joint investigations and joint enforcement measures. Similarly to the mutual assistance procedure, joint operations can be used in the context of cross-border cases subject to the OSS procedure or for national cases with a cross-border component.

In 2019, no joint operations were carried out by SAs.

#### 6.2. NATIONAL CASES<sup>1</sup>

National SAs have different corrective measures at their disposal:

- Issuing warnings to a controller or processor that intended processing operations are likely to infringe the GDPR;
- Issuing reprimands to a controller or processor where processing operations have infringed the GDPR;
- Ordering the controller or processor to comply with a data subject's requests or to bring processing operations into compliance with the GDPR;
- Imposing processing limitations, bans or fines.

##### 6.2.1. Some relevant national cases with exercise of corrective powers

The violations included failure to implement provisions such as privacy by default and design, right to access or right to erasure. Many cases highlighted a lack of proper technical and organisational measures for ensuring data protection, which led to data breaches.

Several significant incidents involved the processing of special categories of data, such as political opinions, credit information or biometric data. The entities fined were from both the private and the public sector.

##### 6.2.1.1. Austria

In 2019, the Austrian SA imposed an administrative fine of EUR 18 million on the Austrian postal service (Österreichische Post AG), ruling that it had violated several provisions of the GDPR.

The violations included processing of special categories of data such as political opinions without explicit consent from data subjects. The Austrian SA found an additional violation related to the processing of package and relocation data for direct marketing purposes.

On 12 February, the Austrian SA imposed an immediate ban on these processing operations and ordered the erasure of the data. This decision was followed by the issuing of the administrative fine on 23 October. In both cases, the decisions have been challenged before the Federal Administrative Court.

On 12 August, the Austrian SA imposed an administrative fine of EUR 55,000 on a controller operating in the medical sector. For more than six months, the controller had neither appointed a data protection officer nor had it carried out a DPIA. In addition, the controller had obliged data subjects to give their consent to non-GDPR compliant data processing and had failed to provide them with information required by Articles 13 and 14 GDPR.

##### 6.2.1.2. Belgium

On 28 May 2019, the Belgian SA imposed its first financial penalty since the GDPR entered into force. The administrative fine amounted to EUR 2,000 and concerned the misuse of personal data for election purposes. In taking this decision, the SA stressed that matters of data protection should be considered especially important in the context of a governmental mandate.

The Belgian SA issued several other fines or reprimands under the GDPR in 2019:

- On 9 July, the SA issued a reprimand to the Federal Public Service for Health after it failed to respond to the exercise of a citizen's right to data access, despite being ordered to do so by the SA. The decision highlighted the lack of internal procedures enabling the institution to meet the GDPR's requirements.

- On 17 September, the SA imposed a fine of EUR 10,000 on a retailer for requesting a customer's electronic identity card in order to create a loyalty card; the amount and nature of data were deemed disproportionate to the purposes of the service.
- On 25 November, the SA imposed a fine of EUR 5,000 on a mayor and a municipal officer in two separate cases. The SA found that they improperly used personal information to send political advertisements as part of a re-election campaign during the 2018 local elections. Again, the SA highlighted how individuals in public office need to behave exemplarily with regard to data protection, since this is vital to preserve citizens' trust in democracy.
- On 17 December, the SA imposed a fine of EUR 15,000 on a website specialized in legal news for their noncompliant cookie management and privacy policy.
- On the same day, the SA ruled that a non-profit association had failed to comply with a data subject's access request. The SA imposed a fine of EUR 2,000 and ordered the association to meet the request.

#### 6.2.1.3. Denmark

While in most EU countries national SAs can issue administrative fines, the rules vary in Estonia and Denmark. Having examined and assessed a case, the Danish SA transfers it to the police, who examine whether there is a basis for a charge. Any financial penalty is then decided in court.

On 25 March 2019, the Danish SA proposed to fine taxi company Taxa 4x35 a total of DKK 1.2 million (over EUR 160,000) for violating the GDPR. This was the first time that the Danish SA proposed a fine under the GDPR.

During a 2018 inspection, the Danish SA found that the company had failed to delete its customers' data, which amounted to over 8 million personal data records.

On 11 June 2019, the Danish SA proposed a fine of DKK 1.5 million (over EUR 200,000) on furniture company IDDesign A/S for failing to delete the data of 385,000 customers. The company had in fact stored this data in an old system, failing to update it when the GDPR entered into force. As a consequence, deadlines for deletion were never set.

#### 6.2.1.4. Finland

On 15 February 2019, the Finnish SA ordered financial credit company Svea Ekonomi to correct its practices for the processing of personal data.

This decision resulted from two cases, the first of which arose from a single data subject's complaint and concerned the personal data used to assess creditworthiness and the data subject's right to inspect this data.

The SA also investigated Svea Ekonomi's notification practices related to the automatic decision-making system used to assess creditworthiness, finding that they did not sufficiently explain the logic for data processing to the extent that a credit applicant could understand the grounds for the decision.

#### 6.2.1.5. France

On 21 January, the French SA (CNIL) imposed a financial penalty of EUR 50 million on Google LLC for lack of transparency, inadequate information and lack of valid consent regarding the personalisation of ads. This was the first time that the CNIL issued a fine under the GDPR.

The case arose from group complaints made by two associations in 2018, which challenged Google's legal basis to process its service users' personal data, particularly for ad personalisation purposes.

As Google has its European headquarters in Ireland, the CNIL contacted the other SAs to assess which Supervisory Authority should be considered the LSA.

The European headquarters of Google did not have decision-making powers on the processing operations in the context of the Android system or the services provided by Google when creating an account during the configuration of a mobile phone. Due to these circumstances, the OSS mechanism was not applicable.

Therefore, the CNIL was able to initiate investigations into the compliance of the processing operations implemented by Google with the French Data Protection Act and the GDPR. The CNIL's restricted committee observed two types of

breaches of the GDPR:

- A violation of the obligations of transparency and information.** The information provided by Google was found to be not easily accessible for users. In addition, some information was not always clear nor comprehensive.
- A violation of the obligation to have a legal basis for data processing for ad personalisation.** It was observed that the users' consent was not sufficiently informed in relation to the extent of data processing. Moreover, the collected consent was neither specific nor unambiguous, as it lacked a clear affirmative action from the user.

The CNIL's restricted committee deemed that these infringements deprived users of essential guarantees regarding processing operations that can reveal important parts of their private life, since they are based on a huge amount of data, a wide variety of services and almost unlimited possible combinations. Moreover, the violations were continuous breaches of the GDPR, rather than one-off, time-limited infringements. In the opinion of the committee, this justified the fine's extent and publicity.

#### 6.2.1.6. Germany

On 30 October 2019, the Berlin SA issued a fine of EUR 14.5 million against Deutsche Wohnen SE for violations of the GDPR. During on-site inspections, the SA found that the company had unnecessarily stored its tenants' personal data without providing the possibility of removing the data. Following a second inspection, the SA found that the company had not made meaningful progress and imposed the fine.

On 3 December, the SA of Rhineland-Palatinate imposed a fine of EUR 105,000 on a hospital for structural technical and organisational deficits in the hospital's patient and privacy management.

At the federal level, the Federal Commissioner for Data Protection and Freedom of Information (BfDI) imposed two fines on telecommunications service providers on 18 December 2019:

- The BfDI imposed a fine of EUR 9,550,000 on 1&1 Telecom GmbH, finding that the company did not

provide sufficient technical and organizational measures to prevent unauthorised persons from being able to obtain customer information via the customer hotline service.

- It also imposed a fine of EUR 10,000 on Rapidata GmbH for failing to appoint an internal data protection officer.

#### 6.2.1.7. Greece

In 2019, the Hellenic SA imposed four administrative fines under the GDPR:

- In July, after an investigation into PricewaterhouseCoopers Business Solutions, the SA found that the company had processed employees' personal data in an unlawful, unfair and non-transparent manner. As a result, the SA imposed a fine of EUR 150,000 and ordered the company to correct its processing operations to comply with the GDPR.
- On 7 October, the SA imposed two administrative fines amounting to a total of EUR 400,000 on telephone service provider Hellenic Telecommunications Organization (OTE), for failure to implement a number of provisions under the GDPR, namely the principle of accuracy, data protection by design and the right to object.
- In December, after an investigation into ALLSEAS MARINE S.A., the SA found that the GDPR had been infringed. The company had failed to comply with a data subject's request to access his personal data stored on a company computer. As a result, the SA ordered the company to comply with the complainant's request immediately. In addition, it ordered the company to ensure within a month that the processing operations via video devices comply with the GDPR and imposed an administrative fine amounting to EUR 15,000 on the company.





- In December, the SA also imposed a fine of EUR 150,000 on AEGEAN MARINE PETROLEUM NETWORK INC (AMPNI) for GDPR violations with regard to personal data processing operations. In addition, the data controller violated the principles of transparency and of secure processing, due to a lack of appropriate technical and organizational measures, which resulted in the unlawful copying of the entire contents of the company's server.

#### 6.2.1.8. Hungary

The Hungarian SA (NAIH) was notified by a citizen that a webpage operated by a Hungarian parliamentary party, the Democratic Coalition (DK), contained personal data of the party's supporters and was openly accessible via an anonymous hacker forum.

Following a data breach during which an unknown attacker uploaded the data on the internet, DK failed to notify the NAIH or the 6,000 data subjects affected by the breach.

The NAIH ruled that the fact that the concerned data were special categories of personal data revealing political opinions was an aggravating circumstance and issued an administrative fine of HUF 11 million (EUR 32,000).

#### 6.2.1.9. Italy

On 30 April 2019, the Italian SA issued a decision against one of Italy's leading email service providers after the company notified a data breach. On 20 February, technical inquiries had spotted fraudulent access via a WiFi hotspot, which had affected about 1.5 million users.

To limit the data breach consequences, the affected users trying to access their accounts were instructed to change their passwords. Affected users received emails with very limited information on unspecified "unusual activities" in the processing systems, without any reference to a data breach or any indication to take additional measures.

The Italian SA considered the information provided to be insufficient, in the light of the severe risks users had

been exposed to, and ordered the company to reissue the communication with a clear description of the type of breach and its possible consequences. The SA also mandated that the company provide users with specific guidance on what measures to take in order to prevent additional risks.

#### 6.2.1.10. Latvia

On 26 August 2019, the Director of the Latvian SA (DSI) imposed a financial penalty of EUR 7,000 against an online retailer for non-compliance with GDPR provisions such as data subjects' right to erasure and non-cooperation with the SA.

The DSI's investigation was initiated after a data subject's complaint that the company had not deleted their personal data despite repeated requests.

#### 6.2.1.11. Lithuania

On 14 May 2019, the Lithuanian SA imposed its first significant fine for breaches of the GDPR. The sanction was imposed on financial services company MisterTango UAB, following a personal data breach in the payment initiation service system, which, among other things, had not been reported to the SA.

As the company owns a branch in Latvia and therefore operates internationally, the Lithuanian SA coordinated with its Latvian counterpart to reach a decision.

Following an investigation, the Lithuanian SA ruled that the company had breached the GDPR's requirements, as it improperly processed personal data in screenshots, made personal data publicly available and failed to report the personal data breach to the SA.

The SA imposed an administrative fine of EUR 61,500. The decision was appealed, but the complaint was rejected by the court of first instance. At the time of publishing this report, the decision was under appeal before the higher court.

#### 6.2.1.12. Malta

In November 2018, the Maltese SA was informed of a

personal data breach on the Lands Authority's online portal, following a report by newspaper The Times of Malta.

The SA's investigation established that the online application platform available on the Authority's portal lacked the necessary technical and organisational measures to ensure secure processing.

On 20 February 2019, the SA found that the Lands Authority had infringed the provisions of the GDPR and issued an administrative fine of EUR 5,000.

#### 6.2.1.13. Norway

On 19 March 2019, the Norwegian SA imposed an administrative fine of NOK 1.6 million, the equivalent of EUR 170,000, on the Municipality of Bergen.

The incident related to computer files in the municipality's computer system, containing the personal data of over 35,000 pupils and employees of the municipality's primary schools. Due to insufficient security measures, these files were unprotected and openly accessible for any system user regardless of type of authorisation.

This enabled unauthorised users to access the school's various information systems and personal data. The fact that the majority of the affected individuals were children and that the municipality was warned several times (both by the authority and by an internal whistleblower) were considered aggravating factors. The municipality did not appeal the decision.

In 2019, the Norwegian SA also imposed two administrative fines on the Municipality of Oslo, which did not appeal their decisions.

- On 11 October, the Municipality's Education Agency was fined EUR 120,000 for failing to implement appropriate security measures in the data processing of a mobile app. The app was used for communication between school employees, parents and pupils.
- On 18 December, the Municipality's Nursing Home Agency was fined EUR 49,300 for having stored patient data from the city's nursing homes and health centres outside the electronic health record system, from 2007 to November 2018.

#### 6.2.1.14. Poland

In 2019, the Polish SA (UODO) issued the following fines under the GDPR:

- On 26 March, the UODO imposed its first fine, amounting to PLN 943,000 (EUR 220,000), for a company's failure to fulfil the information obligation.
- On 20 September, the UODO imposed a fine of PLN 2.8 million (EUR 645,000) on Morele.net for non-compliance with the required technical means of data protection, such as the principle of confidentiality, as set out in Article 5.1.f GDPR.
- On 31 October, the UODO imposed its first administrative fine on a public entity, for an amount of PLN 40,000 (over EUR 9,200). The reason for imposing the fine was that the mayor of the city did not conclude a personal data processing agreement with the entities to which he transferred data.
- On 6 November, the UODO imposed an administrative fine of over PLN 200,000 (over EUR 46,000) on ClickQuickNow for, inter alia, obstructing the exercise of the right to withdraw consent to the processing of personal data.

#### 6.2.1.15. Romania

In 2019, the Romanian SA issued 20 fines for violations of the GDPR:

- On 26 June, the SA issued its first administrative fine under the GDPR, sanctioning bank UniCredit RON 613,912 (EUR 130,000) for its failure to implement appropriate technical and organisational measures to ensure data protection in its processing. As a result, almost 340,000 individuals were exposed to disclosure of their personal data between 25 May and 10 December 2018.
- On 2 July, the SA found that hotel World Trade Center Bucharest had not implemented the necessary measures for secure processing, leading to a leak of clients' personal data. It fined the controller for an amount of RON 71,028 (EUR 15,000).
- On 5 July, the SA fined Legal Company & Tax Hub SRL RON 14,173.50 (EUR 3,000), for failure to implement adequate technical and organisational measures to ensure secure data processing.
- In July, the SA also imposed an administrative fine of

- RON 11,834.25 (EUR 2,500) on Utties Industries SRL, for failure to comply with secure data processing in the context of video devices and employees' personal identification numbers.
- On 28 October, the SA finalised its investigation into controller Fan Courier Express, and found that it did not implement adequate technical and organizational measures to ensure protection of data in its processing. As a result, the company was fined RON 52,325.90 (EUR 11,000).
- On 31 October, the SA imposed three administrative fines. The first, amounting to EUR 9,000, was imposed on Inteligo Media for failing to prove that it had obtained explicit consent for data processing from over 4,000 users. The SA also imposed two fines, EUR 150,000 and EUR 20,000 respectively, on Raiffeisen Bank and Vreau Credit, as it found that the two controllers had unlawfully exchanged clients' personal data in order to determine their eligibility for credit.
- On 4 November, the SA issued a fine against ING Bank's Bucharest branch for failing to ensure compliance with the principles of privacy by design and by default in the settlement process of card transactions affecting over 225,000 customers. The sanction amounted to EUR 80,000.
- On 7 November, air transport company Tarom was fined RON 95,194 (EUR 20,000), due to failure to implement the necessary measures to ensure secure data processing, which resulted in a data breach.
- On 18 November, the SA fined Royal President SRL RON 11,932.25 (EUR 2,500), for failing to grant the right of access within the time limit and for unauthorised disclosure of personal data.
- On 19 November, Globus Score SRL was fined RON 9,551.80 (EUR 2,000) for failing to comply with the SA's request of information, following the opening of an investigation.
- On 25 November, the SA fined Telekom Romania Mobile Communications RON 9,544.40 (EUR 2,000) for failing to keep its customers' personal data accurate, up-to-date and confidential.
- On 29 November, an association of owners was fined RON 2,389.05 (EUR 500) and issued with two reprimands for unlawful accessing personal images from a video surveillance system.

#### 6.2.1.16 Spain

On 17 October, the Spanish SA fined the company Vueling a total of EUR 30,000 for its website cookie policy.

While users accessing the website were informed about the general cookie policy, the company did not provide a management system or cookie configuration panel allowing the user to delete cookies in a granular way. Besides violating the GDPR, these circumstances were also an infringement of the Spanish Law on Information Society Services and Electronic Commerce, which requires that users give explicit consent to any use of data storage and retrieval devices.

#### 6.2.1.17 Sweden

On 22 August 2019, the Swedish SA issued its first financial penalty under the GDPR. The SA fined a municipality SEK 200,000 (approximately EUR 20,000) for using facial recognition technology to monitor school students' attendance.

- On 2 December, the SA issued three administrative fines. The Bucharest branch of BNP Paribas Personal Finance was fined RON 9,508 (EUR 2,000) after complaints that it had failed to delete personal data within the required time limit. The SA also fined controllers Modern Barber SRL and Nicola Medical Team 17 SRL for failing to comply with the SA's request of information. The sanctions amounted to RON 14,329.50 (EUR 3,000) and RON 9,555.40 (EUR 2,000) respectively.
- On 10 December, the SA fined Hora Credit IFN SA a total amount of RON 66,901.80 (EUR 15,000). The controller processed personal data without verifying and validating its accuracy, and failed to maintain its confidentiality.
- On 13 December, company Entirely Shipping & Trading SRL was fined a total amount of RON 47,786 (EUR 10,000) for several violations of the GDPR, including legitimate interest in the context of video surveillance, lack of adequate data protection policies and unlawful processing of biometric data.
- On 16 December, the SA imposed an administrative fine of RON 14,334.30 (EUR 3,000) on SC Enel Energie SA, for failing to comply with the data subject's right to consent and object to the processing of their personal data.

The SA found that the school processed sensitive biometric data unlawfully and failed to conduct an adequate impact assessment, including seeking prior consultation with the SA. In addition, although the processing was based on consent, the SA considered it did not have a valid legal basis given the clear imbalance between the data subject and the controller.

On 18 December 2019, the Swedish SA issued an administrative fine of EUR 35,000 EUR against Mrkoll.se, a website that publishes the personal data of all Swedes above the age of 16 (over 8 million people). In Sweden, websites which are granted publishing certificates have a constitutional protection for the majority of their activities, meaning that the GDPR does not apply under those circumstances.

However, the SA found that some of the data published by the website fell under special categories, such as credit information and criminal records. This required the SA's authorisation, which had not been issued.

#### 6.2.1.18 United Kingdom

On 20 December 2019, the UK SA (ICO) fined a London-based pharmacy GBP 275,000 (EUR 315,000) for failing to ensure the security of special category data.

The pharmacy, Doorstep Dispensaree Ltd, which supplies medicines to customers and care homes, left approximately 500,000 documents in unlocked containers in its premises. The documents included names, addresses, dates of birth, NHS numbers, medical information, and prescriptions belonging to an unknown number of people.

The ICO launched its investigation after it was alerted to the insecurely stored documents by the Medicines and Healthcare Products Regulatory Agency, which was carrying out its own separate enquiry.

In addition to the fine, Doorstep Dispensaree was issued with an enforcement notice due to the significance of the violations and was ordered to improve its data protection practices within three months.

#### **6.3. SA SURVEY ON BUDGET AND STAFF**

Under the GDPR, SAs have received new harmonised tasks and powers. They wield greater enforcement and investigation

powers, handle individuals' complaints, promote awareness on data protection law, and cooperate with the other SAs. This implies a need for increased budgets and more staff members.

In the context of the evaluation of the GDPR, the EDPB conducted a survey among the SAs about their budget and staff. Most of SAs stated that resources made available to them are insufficient.

**The EDPB surveyed Supervisory Authorities in the context of the review of the GDPR. While an increase in the 2019 budget occurred in 27 cases, most SAs found available resources insufficient.**

Based on information provided by SAs from 30 EEA countries, an increase in the budget for 2019 occurred in 27 cases. The remaining three SAs saw their budget decrease. According to the same survey, a majority of SAs (22) increased their staff numbers in 2019. Five SAs reported that the number of their employees did not increase from 2018 to 2019, while three SAs saw a decrease in staff numbers. Differences in personnel requirements across SAs are to be expected, given the varied remits of the SAs.

The EDPB also collected similar information upon request from the European Parliament's LIBE committee. This report is available on the EDPB's [website](#).



# 7



## Coordinated Supervision Committee of the large-scale EU Information Systems and of EU bodies, offices and agencies

In October 2018, [Regulation 2018/1725](#) on the protection of personal data processed by EU institutions and bodies was adopted.

In accordance with Article 62 of this regulation, the European Data Protection Supervisor (EDPS) and the national Supervisory Authorities (SAs) shall cooperate actively to ensure effective supervision of large-scale IT systems and of EU bodies, offices and agencies. For this purpose, the EDPS and SAs shall meet at least twice per year within the framework of the EDPB. Additionally, several legal acts on large-scale IT systems and EU agencies refer to this model of coordinated supervision.

In December 2019, the Coordinated Supervision Committee was formally established within the EDPB. It brings together

EEA SAs and the EDPS as well as SAs from non-EU Schengen Member States, where foreseen under EU law.

The Committee's tasks include, among others, supporting SAs in carrying out audits and inspections, working on the interpretation or application of the relevant EU legal act, studying problems within the exercise of independent supervision or within the exercise of data subject rights, drawing up harmonised proposals for solutions, and promoting awareness of data protection rights.

Participation in the Committee meetings can occur under

various arrangements, depending on the IT system, body, office or agency for which supervision is taking place, as well as the respective EU legal act.

During its first meeting, the Committee elected Giuseppe Busia from the Italian SA as Coordinator and Iris Gnedler from the German Federal SA as Deputy Coordinator for a term of two years, and adopted its Rules of Procedure.

Article 62 of Regulation 2018/1725 outlines the Committee's supervision of IT systems, bodies, offices, and agencies in the following fields:

**1. Border, Asylum and Migration:**

- a. Schengen Information System (SIS), ensuring border control cooperation;
- b. Entry Exit System (EES), which registers entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Schengen States;
- c. European Travel Information and Authorization System (ETIAS), which tracks visitors from countries who do not need a visa to enter the Schengen Zone;
- d. Visa Information System (VIS), connecting consulates in non-EU countries and all external border-crossing points of Schengen States.

**2. Police and Justice Cooperation:**

- a. SIS, which also ensures law enforcement cooperation;
- b. European Public Prosecutor Office (EPPO);
- c. Eurojust, the agency responsible for judicial cooperation in criminal matters among EU Member States;
- d. European Criminal Records Information System on third-country nationals (ECRIS-TCN), which allows Member States' authorities to identify which other Member States hold criminal records on third-country nationals or stateless persons being checked.

**3. Internal Market:** IMI system, which allows exchange of information between public authorities involved in the practical implementation of EU law.

In 2019, the Committee was in charge of the coordinated supervision of the IMI system and Eurojust. In 2020, this will be extended to include EPPO. In the future, all coordinated supervision of large EU information systems, bodies, offices and agencies will gradually be moved to the Committee.





## Main objectives for 2020

### 8.1. LEGAL WORK PLAN

At the beginning of 2019, the EDPB adopted a two-year [work programme](#) for 2019-2020. This is based on the priorities set by all stakeholders, including the EU legislator, as identified by the EDPB members. Three areas of interest were identified, as outlined below.

By the end of 2019, halfway through its work plan, the EDPB made significant progress across its stated objectives and is advancing towards completing them in its second working year.

#### 8.1.1 Guidance

The EDPB will continue issuing Guidelines to ensure consistent interpretation of the GDPR across the EU, enabling stakeholders and Supervisory Authorities (SAs) to apply the GDPR's provisions in a harmonised manner.

In 2019, the EDPB issued guidance related to the provision of online services to data subjects, as well as video devices, search engine delisting and data protection by design and by default.

In 2020, the EDPB will aim to provide guidance on data controllers and processors, data subject rights and the concept of legitimate interest. It will also intensify its work in the context of advanced technologies, such as connected vehicles, blockchain, artificial intelligence, and digital assistants.

In addition to the work outlined in the work plan, in 2020, the EDPB is to provide guidance on the implications for data protection in the context of the fight against COVID-19, both on its own initiative and upon consultation by the European Commission.

### 8.1.2 Advisory role to the European Commission

The EDPB will continue to advise the European Commission on issues such as cross-border e-Evidence data access requests, the revision or adoption of adequacy decisions for data transfers to third countries and any possible revision of the EU-Canada Passenger Name Record (PNR) agreement.

### 8.1.3 Consistency findings

In cross-border cases where consensus between the Lead SA and Concerned SAs within the relevant cooperation procedure cannot be reached, the EDPB will act as a dispute resolution body and issue binding decisions.

In addition, the EDPB will continue to deliver Consistency Opinions to SAs in line with Article 64 GDPR. These include any relevant draft decision from competent SAs on issues such as cross-border data transfers, Binding Corporate Rules and standard or ad-hoc contractual clauses.

The EDPB will also deliver accreditation requirements for code of conduct monitoring bodies, as well as certification bodies to enable the finalisation of the national legal framework and the use of these accountability tools in practice.

### 8.2. COMMUNICATIONS

The EDPB aims to foster full transparency around its work and activities among media, the public and stakeholders within the public and private sectors.

2019 saw an even greater public focus on data protection and privacy issues. The first full year of the GDPR being in application generated considerable discussion among stakeholders and citizens around the importance of data subject rights. It also increased public awareness of issues such as consent, legitimate interest and lawful processing of data.

To respond to this increased level of interest and address stakeholder concerns about the application of the GDPR, the EDPB has been actively engaging with all relevant parties, through workshops, surveys and informational events. In 2020, the EDPB will deepen existing stakeholder relationships and develop new ones.

**The EDPB will continue issuing Guidelines to ensure consistent interpretation of the GDPR, advise the European Commission and deliver Consistency Opinions to Supervisory Authorities.**

The EDPB Members, including its Chair and Deputy Chairs, are fully committed to continuing their participation in relevant conferences and speaking engagements.

The EDPB Secretariat will continue to ensure a harmonised communication approach. This includes continuing to drive public engagement with the EDPB's activities through its social media presence, as well as enhancing cooperation with SAs. To this end, the EDPB will maintain and strengthen the network of SAs' press and communications officers.

# Annexes

## 9.1 GENERAL GUIDANCE ADOPTED IN 2019

- [Recommendation 01/2019 on the draft list of the European Data Protection Supervisor regarding the processing operations subject to the requirement of a data protection impact assessment \(Article 39.4 of Regulation \(EU\) 2018/1725\)](#)
- [Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 - version adopted after public consultation](#)
- [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 adopted after public consultation](#)
- [Guidelines 3/2019 on processing of personal data through video devices – version adopted after public consultation](#)
- [Guidelines 4/2019 on Article 25 Data Protection by Design and by Default – version for public consultation](#)
- [Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR \(part 1\) – version for public consultation](#)

## 9.2 CONSISTENCY OPINIONS ADOPTED IN 2019

- [Opinion 1/2019 on the draft list of the competent supervisory authority of the Principality of Liechtenstein regarding the processing operations subject to the requirement of a data protection](#)
- [Opinion 2/2019 on the competence of a supervisory](#)

## impact assessment (Article 35.4 GDPR)

- [Opinion 2/2019 on the draft list of the competent supervisory authority of Norway regarding the processing operations subject to the requirement of a data protection impact assessment \(Article 35.4 GDPR\)](#)
- [Opinion 4/2019 on the draft Administrative Arrangement for the transfer of personal data between European Economic Area \("EEA"\) Financial Supervisory Authorities and non-EEA Financial Supervisory Authorities](#)
  - [Draft administrative arrangement for the transfer of personal data](#)
- [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](#)
- [Opinion 6/2019 on the draft list of the competent supervisory authority of Spain regarding the processing operations subject to the requirement of a data protection impact assessment \(Article 35.4 GDPR\)](#)
- [Opinion 7/2019 on the draft list of the competent supervisory authority of Iceland regarding the processing operations subject to the requirement of a data protection impact assessment \(Article 35.4 GDPR\)](#)
- [Opinion 8/2019 on the competence of a supervisory](#)

[authority in case of a change in circumstances relating to the main or single establishment](#)

- [Opinion 9/2019 on the Austrian data protection supervisory authority draft accreditation requirements for a code of conduct monitoring body pursuant to article 41 GDPR](#)
- [Opinion 10/2019 on the draft list of the competent supervisory authority of Cyprus regarding the processing operations subject to the requirement of a data protection impact assessment \(Article 35\(4\) GDPR\)](#)
- [Opinion 11/2019 on the draft list of the competent supervisory authority of the Czech Republic regarding the processing operations exempt from the requirement of a data protection impact assessment \(Article 35\(5\) GDPR\)](#)
- [Opinion 12/2019 on the draft list of the competent supervisory authority of Spain regarding the processing operations exempt from the requirement of a data protection impact assessment \(Article 35\(5\) GDPR\)](#)
- [Opinion 13/2019 on the draft list of the competent supervisory authority of France regarding the processing operations exempt from the requirement of a data protection impact assessment \(Article 35\(5\) GDPR\)](#)
- [Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA \(Article 28\(8\) GDPR\)](#)
  - [DK SA Standard Contractual Clauses for the purposes of compliance with art. 28 GDPR](#)
- [Opinion 15/2019 on the draft decision of the competent supervisory authority of the United Kingdom regarding the Binding Corporate Rules of Equinix Inc.](#)

- [Opinion 16/2019 on the draft decision of the Belgian Supervisory Authority regarding the Binding Corporate Rules of ExxonMobil Corporation](#)
- [Opinion 17/2019 on the UK data protection supervisory authority draft accreditation requirements for a code of conduct monitoring body pursuant to article 41 GDPR](#)

## 9.3 JOINT OPINIONS ADOPTED IN 2019

- [EDPB-EDPS Joint Opinion 1/2019 on the processing of patients' data and the role of the European Commission within the eHealth Digital Service Infrastructure \(eHDSI\)](#)

## 9.4 LEGISLATIVE CONSULTATION

- [Second Annual Joint Review report on the EU-US Privacy Shield](#)
- [Third Annual Joint Review report on the EU-US Privacy Shield](#)
- [Opinion 3/2019 on the interplay between the Clinical Trials Regulation \(CTR\) and the GDPR](#)
- [Statement 3/2019 on an ePrivacy regulation](#)
- [Contribution to the draft second additional protocol to the Council of Europe Convention on Cybercrime \(Budapest Convention\)](#)

## 9.5 OTHER DOCUMENTS

- [Information note on data transfers under the GDPR in the event of a no-deal Brexit](#)
- [Statement 1/2019 on the US Foreign Account Tax Compliance Act \(FATCA\)](#)
- [EDPB LIBE report on the implementation of GDPR](#)
- [EDPB pleading before the CJEU in Case C-311/18 \(Facebook Ireland and Schrems\)](#)

## 9.6. LIST OF EXPERT SUBGROUPS WITH SCOPE OF MANDATE

NAME OF SUBGROUP	SCOPE OF MANDATE	NAME OF SUBGROUP	SCOPE OF MANDATE
<b>Borders, Travel &amp; Law Enforcement (BTLE) Expert Subgroup</b>	<ul style="list-style-type: none"> <li>• Law enforcement directive</li> <li>• Cross-border requests for e-evidence</li> <li>• Adequacy Decisions, access to transferred data by law enforcement and national intelligence authorities in third countries (e.g. EU-US Privacy Shield)</li> <li>• Passenger Name Records (PNR)</li> <li>• Border controls</li> <li>• Preparation of the coordinated supervision under Art. 62 1725/2018</li> </ul>	<b>Enforcement Expert Subgroup</b>	<ul style="list-style-type: none"> <li>• Mapping/analysing the need for additional clarifications or guidance, based on practical experiences with the application of Chapters VI, VII and VIII GDPR</li> <li>• Mapping/analysing possible updates of existing Cooperation subgroup tools</li> <li>• Monitoring of investigation activities</li> <li>• Practical questions on investigations</li> <li>• Guidance on the practical application of Chapter VII GDPR including exchanges on concrete cases</li> <li>• Guidance on the application of Chapter VIII GDPR together with the Fining TF</li> </ul>
<b>Compliance, e-Government and Health Expert Subgroup</b>	<ul style="list-style-type: none"> <li>• Code of conduct, certification and accreditation</li> <li>• Close cooperation on DPIA with the Technology ESG focusing on the perspective of their mandates</li> <li>• Close cooperation on privacy by design and by default with the Technology ESG focusing on the perspective of their mandates</li> <li>• Compliance with public law and eGovernment</li> <li>• Health</li> </ul>	<b>Financial Matters Expert Subgroup</b>	<ul style="list-style-type: none"> <li>• Application of data protection principles in the financial sector (e.g. automatic exchange of personal data for tax purposes; impact of FATCA on the protection of personal data; interplay between Second Payment Services Directive and GDPR)</li> </ul>
<b>Cooperation Expert Subgroup</b>	<ul style="list-style-type: none"> <li>• General focus on procedures of the GDPR</li> <li>• Guidance on procedural questions</li> <li>• International mutual assistance and other cooperation tools to enforce the GDPR outside the EU (Art. 50 GDPR)</li> </ul>	<b>International Transfers Expert Subgroup</b>	<p>Guidance on Chapter V (International transfer tools and policy issues), more specifically:</p> <ul style="list-style-type: none"> <li>• Review European Commission Adequacy decisions</li> <li>• Guidelines on Art. 46 GDPR and review of administrative arrangements between public authorities and bodies (e.g. ESMA)</li> <li>• Codes of conduct and certification as transfer tools</li> <li>• Art. 48 GDPR together with BTLE ESG</li> <li>• Art. 50 GDPR together with Cooperation ESG</li> <li>• Guidelines on territorial scope and the interplay with Chapter V of the GDPR - interaction with Key Provisions ESG</li> <li>• Exchange of information on review of BCRs and ad hoc contractual clauses according to Art. 64 GDPR</li> </ul>
<b>Coordinators Expert Subgroup</b>	<ul style="list-style-type: none"> <li>• General coordination between the Expert Subgroup Coordinators</li> <li>• Coordination on the annual Expert Subgroup working plan</li> </ul>		

NAME OF SUBGROUP	SCOPE OF MANDATE	NAME OF SUBGROUP	SCOPE OF MANDATE
<b>IT Users Expert Subgroup</b>	<p>Developing and testing IT tools used by the EDPB with a practical focus:</p> <ul style="list-style-type: none"> <li>• Collecting feedback on the IT system from users</li> <li>• Adapting the systems and manuals</li> <li>• Discussing other business needs including tele- and videoconference systems</li> </ul>	<b>Strategic Advisory Expert Subgroup</b>	<ul style="list-style-type: none"> <li>• Guidance on strategic questions affecting the whole EDPB (including the discussion on the work plans of the ESGs)</li> <li>• Clarification of questions that could not be resolved in the ESG</li> </ul>
<b>Key Provisions Expert Subgroup</b>	Guidance on core concepts and principles of the GDPR, including Chapters I (e.g. scope, definitions like LSA and large scale processing) and II (main principles); Chapters III (e.g. rights of individuals, transparency), IV (e.g. DPO – shared competences with Compliance Tools ESG, Enforcement ESG and Technology ESG) and IX	<b>Taskforce on Administrative Fines</b>	Development of Guidelines on the harmonisation of the calculation of fines
<b>Social Media Expert Subgroup</b>	<ul style="list-style-type: none"> <li>• Analyzing social media services, conceived as online platforms that focus on enabling the development of networks and communities of users, among which information and content is shared and whereby additional functions provided by social media services include targeting, personalisation, application integration, social plug-ins, user authentication, analytics and publishing</li> <li>• Analysing established and emerging functions offered by social media, including the underlying processing activities and corresponding risks for the rights and freedoms of individuals</li> <li>• Developing guidance, recommendations and best practices in relation to both the offer and use of social media functions, in particular for economic or political reasons.</li> <li>• Providing assistance to other subgroups, in particular by proposing strategic priorities in terms of (a) supervision and (b) the development of new EDPB guidance or updating of existing WP29 guidance</li> </ul>	<b>Technology Expert Subgroup</b>	<ul style="list-style-type: none"> <li>• Technology, innovation, information security, confidentiality of communication in general</li> <li>• ePrivacy, encryption</li> <li>• DPIA and data breach notifications</li> <li>• Emerging technologies, innovation and other challenges related to privacy: reflecting on data protection risks of future technological developments</li> <li>• Providing input on technology matters relevant to other ESGs</li> </ul>

# Contact details

**Postal address:**

Rue Wiertz 60, B-1047 Brussels

**Office address:**

Rue Montoyer 30, B-1000 Brussels

**Email:**

[edpb@edpb.europa.eu](mailto:edpb@edpb.europa.eu)

-  @eu\_edpb
-  eu-edpb
-  edpb.europa.eu



European Data Protection Board

# 2021 ANNUAL REPORT

Enhancing the depth  
and breadth of  
data protection



# ENHANCING THE DEPTH AND BREADTH OF DATA PROTECTION

An Executive Summary of this report, which provides an overview of key EDPB activities in 2021, is also available.

Further details about the EDPB can be found on our website at [edpb.europa.eu](http://edpb.europa.eu).

# TABLE OF CONTENTS

1  
2  
3

<b>GLOSSARY</b>	<b>7</b>	3.3.2. EDPS-EDPB Joint Opinion 02/2021 on standard contractual clauses for the transfer of personal data to third countries	16
<b>FOREWORD</b>	<b>10</b>		
<b>2021 - HIGHLIGHTS</b>	<b>13</b>	3.4. EDPB-EDPS JOINT OPINION 05/2021 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
3.1. STRATEGY 2021-2023 AND WORK PROGRAMME 2021-2022	13	3.5. BINDING DECISION 01/2021 ON THE DISPUTE ARISING ON THE DRAFT DECISION OF THE IRISH SUPERVISORY AUTHORITY REGARDING WHATSAPP IRELAND UNDER ART. 65(1)(A) GDPR	19
3.2. EDPB OPINIONS ON DRAFT UK ADEQUACY DECISIONS	13	3.6. URGENT BINDING DECISION 01/2021 ON THE REQUEST UNDER ART. 66(2) GDPR FROM THE HAMBURG (GERMAN) SUPERVISORY AUTHORITY FOR ORDERING THE ADOPTION OF FINAL MEASURES REGARDING FACEBOOK IRELAND LIMITED	20
3.2.1. Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive	14		
3.2.2. Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom	15		
3.2.3. Opinion 15/2021 regarding the European Commission Draft Implementing Decision pursuant to Directive (EU) 2016/680 on the adequate protection of personal data in the United Kingdom	16		
3.3. FURTHER GUIDANCE AND OPINIONS FOLLOWING THE CASE C-311/18 SCHREMS II RULING BY THE CJEU	16	4.1. THE EDPB SECRETARIAT	22
3.3.1. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data – Version 2.0	16	4.2. THE EDPB SECRETARIAT'S CONTRIBUTION TO THE NATIONAL SAs' COOPERATION	23
		4.3. IT COMMUNICATIONS TOOL (INTERNAL MARKET INFORMATION) AND THE NEW EDPB WEBSITE	23
		4.4. THE EDPB SECRETARIAT'S ACTIVITIES RELATING TO ACCESS TO DOCUMENTS	24
		4.5. THE EDPB SECRETARIAT'S ACTIVITIES RELATING TO DATA PROTECTION OFFICER ACTIVITIES	25
		<b>2021 - THE EDPB SECRETARIAT</b>	<b>22</b>

<b>5</b>	<b>EUROPEAN DATA PROTECTION BOARD - ACTIVITIES IN 2021</b>	<b>26</b>			
5.1.	GENERAL GUIDANCE (GUIDELINES AND RECOMMENDATIONS)	26	5.2.2.	Opinions on draft requirements for accreditation of a certification body	35
5.1.1.	Guidelines 01/2021 on examples regarding personal data breach notification	27	5.2.3.	Opinions on SAs' approval of accreditation requirements for code of conduct monitoring body	36
5.1.2.	Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive	27	5.2.4.	Opinion on SAs' draft Standard Contractual Clauses	36
5.1.3.	Guidance Addendum on certification criteria assessment (Addendum to Guidelines 1/2018 on certification and identifying certification criteria in accordance with Arts. 42 and 43 GDPR)	28	5.2.5.	Opinions on SAs' approval of codes of conduct	37
5.1.4.	Guidelines 02/2021 on virtual voice assistants	28	5.2.6.	Opinion on SAs' authorisation of administrative arrangements	37
5.1.5.	Guidelines 03/2021 on the application of Art. 65(1)(a) GDPR	29	5.2.7.	Opinion on the legal basis for an SA to order ex officio data erasure	37
5.1.6.	Recommendations 02/2021 on the legal basis for the storage of credit card data for the sole purpose of facilitating further online transactions	29	5.3.	<b>BINDING DECISIONS</b>	38
5.1.7.	Guidelines 04/2021 on codes of conduct as tools for transfers	29	5.3.1.	Binding Decision 01/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Art. 65(1)(a) GDPR	38
5.1.8.	Guidelines 05/2021 on the Interplay between the application of Art. 3 and the provisions on international transfers as per Chapter V of the GDPR	30	5.3.2.	Urgent Binding Decision 01/2021 on the request under Art. 66(2) GDPR from the Hamburg (German) Supervisory Authority for ordering the adoption of final measures regarding Facebook Ireland Limited	38
5.1.9.	Guidelines adopted after public consultation	31	5.4.	<b>REGISTER FOR DECISIONS TAKEN BY SUPERVISORY AUTHORITIES AND COURTS ON ISSUES HANDLED IN THE CONSISTENCY MECHANISM</b>	38
5.2.	<b>CONSISTENCY OPINIONS</b>	<b>33</b>	5.5.	<b>LEGISLATIVE CONSULTATION AND DOCUMENTS ADDRESSED TO THE EUIS OR NATIONAL AUTHORITIES</b>	39
5.2.1.	Opinions on draft decisions regarding Binding Corporate Rules	33			

<b>5.5.1.</b>	<b>Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom</b>	<b>39</b>	<b>5.5.8.</b>	<b>EDPB-EDPS Joint Opinion 04/2021 on the Proposal for a Regulation of the European Parliament and of the Council on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery to facilitate free movement during the COVID 19 pandemic (Digital Green Certificate)</b>	<b>42</b>
<b>5.5.2.</b>	<b>Opinion 15/2021 regarding the European Commission Draft Implementing Decision pursuant to Directive (EU) 2016/680 on the adequate protection of personal data in the United Kingdom</b>	<b>39</b>	<b>5.5.9.</b>	<b>EDPB-EDPS Joint Opinion 05/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)</b>	<b>43</b>
<b>5.5.3.</b>	<b>Opinion 20/2021 on Tobacco Traceability System</b>	<b>39</b>	<b>5.5.10.</b>	<b>Statement 02/2021 on new draft provisions of the Second Additional Protocol to the Council of Europe Convention on Cybercrime (Budapest Convention)</b>	<b>43</b>
<b>5.5.4.</b>	<b>Opinion 32/2021 regarding the European Commission draft implementing decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the Republic of Korea</b>	<b>40</b>	<b>5.5.11.</b>	<b>Statement 03/2021 on ePrivacy Regulation</b>	<b>44</b>
<b>5.5.5.</b>	<b>EDPB-EDPS Joint Opinion 01/2021 on standard contractual clauses between controllers and processors</b>	<b>41</b>	<b>5.5.12.</b>	<b>Statement 04/2021 on international agreements including transfers</b>	<b>44</b>
<b>5.5.6.</b>	<b>EDPB-EDPS Joint Opinion 02/2021 on standard contractual clauses for the transfer of personal data to third countries</b>	<b>41</b>	<b>5.5.13.</b>	<b>EDPB contribution to the 6th round of consultations on the draft Second Additional Protocol to the Council of Europe Budapest Convention on Cybercrime</b>	<b>44</b>
<b>5.5.7.</b>	<b>EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act)</b>	<b>42</b>	<b>5.5.14.</b>	<b>Statement 05/2021 on the Data Governance Act in light of the legislative developments</b>	<b>45</b>
			<b>5.5.15.</b>	<b>EDPB contribution to the 6th round of consultations on the draft Second Additional Protocol to the Council of Europe Budapest Convention on Cybercrime</b>	<b>45</b>

<b>6.</b>	<b>SUPERVISORY AUTHORITY - ACTIVITIES IN 2021</b>	<b>50</b>		
<b>6.1.</b>	<b>CROSS-BORDER COOPERATION</b>	<b>50</b>		
6.1.1.	Preliminary procedure to identify the Lead and Concerned Supervisory Authorities	50		
6.1.2.	Database regarding cases with a cross-border component	51		
<b>6.6.</b>	<b>OTHER GUIDANCE AND INFORMATION NOTES</b>	<b>45</b>		
5.6.1.	Pre-GDPR BCRs overview list	45	6.1.3.	One-Stop-Shop mechanism and decisions
5.6.2.	Statement on the withdrawal of the United Kingdom from the European Union - update 13/01/2021	46	6.1.4.	Mutual assistance
5.6.3.	Information note on data transfers under the GDPR to the United Kingdom after the transition period - update 13/01/2021	46	6.1.5.	Joint operations
<b>5.7.</b>	<b>PLENARY MEETINGS AND SUBGROUPS</b>	<b>46</b>	<b>6.2.</b>	<b>NATIONAL CASES</b>
<b>5.8.</b>	<b>STAKEHOLDER CONSULTATION</b>	<b>47</b>	6.2.1.	Some relevant national cases with exercise of corrective powers
5.8.1.	Stakeholder events	47	<b>6.3.</b>	<b>SA BUDGET AND STAFF</b>
5.8.2.	Public consultation on draft guidance	47		
5.8.3.	Survey on practical application of adopted guidance	48		
<b>5.9.</b>	<b>EXTERNAL REPRESENTATION OF THE BOARD</b>	<b>49</b>	<b>7</b>	<b>COORDINATED SUPERVISION COMMITTEE OF THE LARGE EU INFORMATION SYSTEMS AND OF EU BODIES, OFFICES AND AGENCIES</b>
5.9.1.	Participation of Chair and Deputy Chairs in conferences and speaking engagements	49		
5.9.2.	Participation of EDPB Staff in conferences and speaking engagements	49	<b>8</b>	<b>ANNEXES</b>
<b>6.1.</b>	<b>CROSS-BORDER COOPERATION</b>	<b>50</b>	8.1.	<b>GENERAL GUIDANCE ADOPTED IN 2021</b>
6.1.1.	Preliminary procedure to identify the Lead and Concerned Supervisory Authorities	50	8.2.	<b>CONSISTENCY OPINIONS AND DECISIONS ADOPTED IN 2021</b>
6.1.2.	Database regarding cases with a cross-border component	51	8.3.	<b>JOINT OPINIONS ADOPTED IN 2021</b>
6.1.3.	One-Stop-Shop mechanism and decisions	51	8.4.	<b>LEGISLATIVE CONSULTATION</b>
6.1.4.	Mutual assistance	66	8.5.	<b>OTHER DOCUMENTS</b>
6.1.5.	Joint operations	66	8.6.	<b>LIST OF EXPERT SUBGROUPS WITH SCOPE OF MANDATES</b>
				<b>84</b>
				<b>87</b>
				<b>88</b>
				<b>90</b>
				<b>90</b>
				<b>90</b>
				<b>91</b>

## 1

# GLOSSARY

<b>Adequacy decision</b>	An implementing act adopted by the European Commission that decides that a non-EU country ensures an adequate level of protection of personal data.
<b>Binding Corporate Rules (BCRs)</b>	Data protection policies adhered to by controller or processors established in the EU for transfers of personal data to controllers or processors outside the EU within a group of undertakings or enterprises or groups of enterprises engaged in a joint economic activity.
<b>Charter of Fundamental Rights of the EU</b>	A legally binding Charter that sets out the civil, political, economic, social and cultural rights of EU citizens and residents (including the right to the protection of personal data in its Art. 8).
<b>Concerned Supervisory Authorities (CSAs)</b>	A Supervisory Authority concerned by the processing of personal data because: (a) the controller or processor is established on the territory of its Member State; (b) data subjects residing in the Member State are substantially affected by the processing; or (c) a complaint has been lodged with that Supervisory Authority.
<b>Court of Justice of the European Union (CJEU)</b>	The highest court in the EU judiciary system, which ensures uniform interpretation and application of EU law in EU Member States. It ensures those States and EU institutions abide by EU law.
<b>Cross-border processing</b>	Either (a) processing of personal data that takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or (b) processing of personal data that 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.
<b>Data controller</b>	The natural or legal person, public authority, agency or other body that, 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 EU or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
<b>Data minimisation</b>	A principle that means that a data controller should limit the collection of personal data to what is directly adequate, relevant and limited to what is necessary to accomplish a specified purpose of the processing.

<b>Data processor</b>	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
<b>Data Protection Impact Assessment (DPIA)</b>	A privacy-related impact assessment aiming to evaluate the processing of personal data, including notably its necessity and proportionality, an assessment of the risks for the rights and freedom of individuals, and the measures envisaged to address the risks.
<b>Data Protection Officer (DPO)</b>	An expert on data protection law and practices, who operates independently within an organisation to ensure the internal application of data protection.
<b>Data subject</b>	The person whose personal data is processed.
<b>European Commission</b>	An EU institution that shapes the EU's overall strategy, proposes new EU laws and policies, monitors their implementation and manages the EU budget.
<b>European Economic Area (EEA) Member States</b>	EU Member States and Iceland, Liechtenstein and Norway.
<b>European Union (EU)</b>	An economic and political union between 27 European countries.
<b>General Data Protection Regulation (GDPR)</b>	An EU Regulation that sets out rules on the rights of data subjects, the duties of data controllers and processors processing personal data, international data transfers and the powers of Supervisory Authorities.
<b>Lead Supervisory Authority (LSA)</b>	The Supervisory Authority where the “main establishment” of a data controller or processor is based, which has the primary responsibility for dealing with a cross-border data processing activity and for coordinating any cross-border investigation.
<b>Main establishment</b>	Either (a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment; or (b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under the GDPR.

<b>One-Stop-Shop mechanism</b>	A mechanism whereby the Supervisory Authority with the “main establishment” of a controller or processor in the EU serves as the Lead Supervisory Authority to ensure cooperation between Supervisory Authorities in the case of cross-border processing.
<b>Personal data</b>	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.
<b>Processing</b>	Any operations or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
<b>Standard Contractual Clauses (SCCs)</b>	A set of contractual clauses that provide adequate safeguards for data transfers from the EU or the EEA to third countries or govern the relationship between controller and processor.
<b>Supervisory Authority (SA)</b>	An independent public supervisory body that monitors the application of the GDPR and other national laws relating to data protection, in order to protect the rights and freedoms of natural persons in relation to the processing of personal data. Also known as a Data Protection Authority (DPA).
<b>Third country</b>	A country outside the EU or EEA.

# 2

## FOREWORD



2021 was the fourth year of existence and the first year of the multiannual EDPB Strategy 2021–2023. It was a very productive year, in which we completed many key actions to reach the objectives set out in our Strategy.

Though we continued to work mostly remotely due to the continuing impact of the COVID-19 pandemic, we made significant progress on a number of important files. To make this possible, we held over 380 EDPB meetings. Here, I outline some highlights from our work over the past year.

Firstly, the EDPB continued to pay a great deal of attention to international transfers of personal data. In 2021, we adopted the final version of our Recommendations on supplementary measures following the *Schrems II* ruling by the Court of Justice of the EU, taking on board the input received from stakeholders during public consultation. These recommendations lay out a clear roadmap of steps data exporters can follow to identify and implement appropriate supplementary measures to ensure an essentially equivalent level of protection for the personal data they transfer to third countries.

The EDPB also adopted Opinions on the UK draft adequacy decisions. While adequacy findings are available to those countries that meet the relevant criteria, EU data protection legislation offers other transfer mechanisms. In line with this, we adopted Guidelines on codes of conduct as tools for transfers. In addition, we issued a Joint Opinion together with the EDPS on a new set of Standard Contractual Clauses (SCCs) issued by the European Commission for the transfer of personal data to controllers and processors established outside the EEA. We worked closely together with the European Commission to ensure full consistency between the SCCs and our Recommendations on supplementary measures.

A second area in which we carried out important work in 2021 was digital policy. In the framework of the EU’s Digital Strategy, the European Commission put forward several proposals on which the EDPB, together with the European Data Protection Supervisor (EDPS), issued legislative advice. The EDPB and EDPS adopted a Joint Opinion on the proposal for a Data Governance Act (DGA) and a statement on the Digital Service Package and Data Strategy. We also adopted an important Joint Opinion with the EDPS on the draft Artificial Intelligence Act. It is crucial that the future DGA and data processing acts under the Artificial Intelligence Act are fully in line with EU personal data protection legislation.

Law enforcement was a third priority area that underscored our work in 2021. Adequacy decisions may also be adopted in the framework of the Law Enforcement Directive (LED). Last year, we adopted recommendations on the LED adequacy referential. By detailing the core data protection principles that have to be present in the third country legal framework to ensure essential equivalence with the EU framework, our guidance aims to standardise the adequacy procedure under the LED. We also carried out an evaluation of the LED itself.

Throughout 2021, we issued several guidance documents to clarify the terms of European data protection law for companies and organisations. For example, we published examples of data breach notifications and guidance on virtual voice assistants. We also adopted the final version of our Guidelines on the concepts of controller and processor and Guidelines on the targeting of social media users, after incorporating stakeholders’ feedback. By interacting and consulting with stakeholders, we aim to make our guidance practical and concrete, answering the needs identified by our stakeholders.

Naturally, a topic that is high on our priority list is the enforcement of the GDPR. So far, the national Supervisory Authorities have worked or are working together on almost 2,000 cross-border cases. The dispute resolution mechanism under Art. 65 GDPR has been triggered twice (once in 2020 and once in 2021) and, in 2021, we also dealt with our first Art. 66 GDPR urgency procedure relating to national provisional measures imposed in Germany against WhatsApp data-sharing practices with Facebook.

In the coming year we will continue to develop guidance to help stakeholders understand and interpret the GDPR. We have set out ambitious goals for 2022, including work on guidance on topics as varied as legitimate interest as a legal basis and the use of facial recognition by law enforcement authorities.

In 2022, we will also continue our work to optimise cooperation and enforcement. A dedicated meeting at the level of the heads of the Supervisory Authorities (SAs) will allow them to share experiences and discuss practical ways to ensure effective and efficient cooperation among SAs.

We see our internal discussions against the backdrop of a broader international debate on cooperation and we aim to invest further resources in the global dimension of data protection. We make a continuous effort to meet and exchange good practices with our colleagues worldwide, through fora such as the Global Privacy Assembly and the G7.

Undoubtedly, the depth and breadth of our work is all thanks to the efforts of everyone within the EDPB, accompanied by the valuable collaborative input and engagement of all stakeholders in our consultations and events.

**Andrea Jelinek**

Chair of the European Data Protection Board

# 3



## 2021 - HIGHLIGHTS

### 3.1. STRATEGY 2021-2023 AND WORK PROGRAMME 2021-2022

In early 2021, the EDPB adopted its two-year Work Programme for 2021-2022, according to Art. 29 of the EDPB Rules of Procedure. The work programme follows the priorities set out in the [Strategy for 2021-2023](#) and will put these into practice.

This Strategy includes four main pillars, as well as a set of three key actions per pillar to help achieve these goals. The pillars and key actions are illustrated below.

The EDPB Strategy and Work Programme will help guide the EDPB's work in 2021 and the years to come. The tools included in the Work Programme will help create a more consistent understanding of the key concepts and processes in the GDPR

and the cooperation and consistency mechanism in particular. This will allow the EDPB to reinforce its leadership in ensuring consistency across the EEA and further drive EEA SAs to work in one direction and to speak in one voice.

### 3.2. EDPB OPINIONS ON DRAFT UK ADEQUACY DECISIONS

The EDPB issued two opinions on the European Commission draft Implementing Decisions on the adequate protection of personal data in the UK. [Opinion 14/2021](#) is based on the GDPR and assesses both general data protection aspects and government access to personal data transferred from the EEA for the purposes of law enforcement and national security included in the draft adequacy decision. [Opinion 15/2021](#) is

## PILLAR 1



### Advancing harmonisation and facilitating compliance

Key notions of Data Protection law:

- Guidelines on data subject rights
- Guidelines on legitimate interest

Ensuring consistency between data protection authorities

Advise the EU legislator on important data protection issues

Awareness-raising common tools on GDPR for SMEs

## PILLAR 2



### Supporting effective enforcement and efficient cooperation between SAs

Consistent application of GDPR cooperation mechanisms:

- Guidance on One-Stop-Shop procedure, Mutual assistance and EDPB decisions relating to dispute resolution
- Guidelines on administrative fines
- Implement a Coordinated Enforcement Framework and a Support Pool of Experts to promote solidarity between authorities and sharing of experts

## PILLAR 3



### A fundamental rights approach to new technologies



New technologies:

- Guidelines on the use of facial recognition technology in the area of law enforcement
- Guidelines on Blockchain
- Guidelines on anonymisation and pseudonymisation
- ePrivacy Regulation

## PILLAR 4



### The global dimension



Promote high standards for international data transfers:

- Adequacy decisions (both under GDPR and LED)
- Codes of Conduct and certification as tools for international transfers

based on the Law Enforcement Directive (LED) and analyses the draft adequacy decision in the light of Recommendations 01/2021 on the adequacy referential under the LED (see Section 5.1.2 of this Report), as well as the relevant case law reflected in Recommendations 02/2020 on the European Essential Guarantees for surveillance measures. This is the first draft implementing decision on a third country's adequacy under the LED ever presented by the European Commission and assessed by the EDPB.

### 3.2.1. Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive

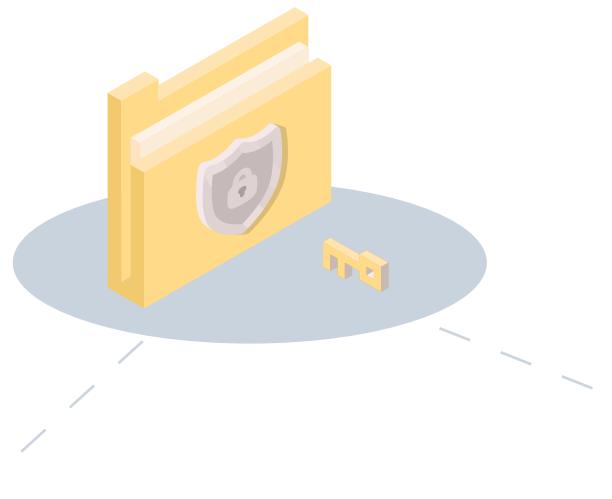
The EDPB issued recommendations to provide guidance to the European Commission on the level of data protection in third countries and international organisations under the LED. The finding of an adequate level of data protection does not need to demonstrate a point-by-point mirroring of EU legislation, but rather that the core requirements of legislation in a third country are effective (i.e. enforced and followed in practice) in ensuring a level of protection in the third country essentially equivalent to that guaranteed in the EU.

To be able to properly advise the European Commission pursuant to Art. 51(1)(g) LED on adequacy decisions, the EDPB should receive all relevant documentation, including relevant correspondence and the findings made by the European Commission, so it can assess the European Commission's analysis. The EDPB should also be kept informed of periodic reviews of adequacy decisions under Art. 36(5) LED and of any action by the European Commission to repeal, amend or suspend adequacy decisions.

As part of an assessment of the level of data protection offered by a third country or international organisation, consideration should be given to:

- The consistency of general principles and safeguards with EU data protection law;
- Principles applied to the processing of special categories of data, automated decision making and profiling, and the application of the principles of data protection by design and default;
- Procedural and enforcement mechanisms in the third country or international organisation;
- Whether the guarantees set out in the EDPB's *Recommendations 02/2020* have been taken into account in the third country or international organisation when assessing the adequacy of a third country under the LED in the field of surveillance.

Adopted: 2 February 2021



### 3.2.2. **Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom**

When providing an assessment of the draft implementing decision on the adequacy of personal data protection offered by the UK under the GDPR, the EDPB finds that many aspects of the UK's data protection framework are essentially equivalent to those in the EU. The EDPB welcomes the UK's continued adherence to the European Convention on Human Rights and Council of Europe Convention 108, and current work on ratifying Convention 108+.

However, there are several potential challenges to seeing the UK's data protection framework as essentially equivalent to that of the EU, including:

- Future possible divergences between UK legal framework and EU data protection law, which require close monitoring by the European Commission;
- The broad formulation of an "immigration exemption" to the application of data subject rights;
- The risk of onward transfer from the UK of personal data received from the EEA to third countries that might undermine the level of protection of the personal data if the rules applicable in the UK to onward transfers do not ensure that an essentially equivalent level of protection will continue to be provided;
- The potential impact of international agreements facilitating access to personal data in the UK by public authorities in third countries.

Due to the potential for the UK to diverge from EU data protection law, the EDPB welcomes the inclusion of a sunset clause, and invites the Commission to monitor closely all relevant developments in the UK that may have an impact on

the essential equivalence of the level of protection of personal data and, where necessary, to take swiftly appropriate actions, such as suspending, amending or repealing the adequacy decision.

Adopted: 13 April 2021

### **3.2.3. Opinion 15/2021 regarding the European Commission Draft Implementing Decision pursuant to Directive (EU) 2016/680 on the adequate protection of personal data in the United Kingdom**

In considering the Commission's draft decision on the adequacy of personal data protection under the LED, the EDPB recognises that many aspects of its data protection framework are essentially equivalent to the protections offered in the EU. The EDPB welcomes the UK's continued adherence to the European Convention on Human Rights and Council of Europe Convention 108, and current work on ratifying Convention 108+.

Noting the possibility that the UK deviates in the future from the EU data protection framework, the EDPB welcomes the addition of a sunset clause into the draft decision. The EDPB highlights the importance of the Commission closely monitoring developments in the UK's data protection framework such as international agreements between the UK and third countries or adequacy decisions adopted by the UK based on standards diverging from the EU's that may undermine the essentially equivalent level of protection of personal data transferred from the EU. Should there be developments entailing that an adequate level of protection can no longer be ensured in the UK, the EDPB recommends to the Commission that the adequacy decision is suspended, amended or repealed, as appropriate.

Adopted: 13 April 2021

### **3.3. FURTHER GUIDANCE AND OPINIONS FOLLOWING THE CASE C-311/18 *SCHREMS II* RULING BY THE CJEU**

#### **3.3.1. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data – Version 2.0**

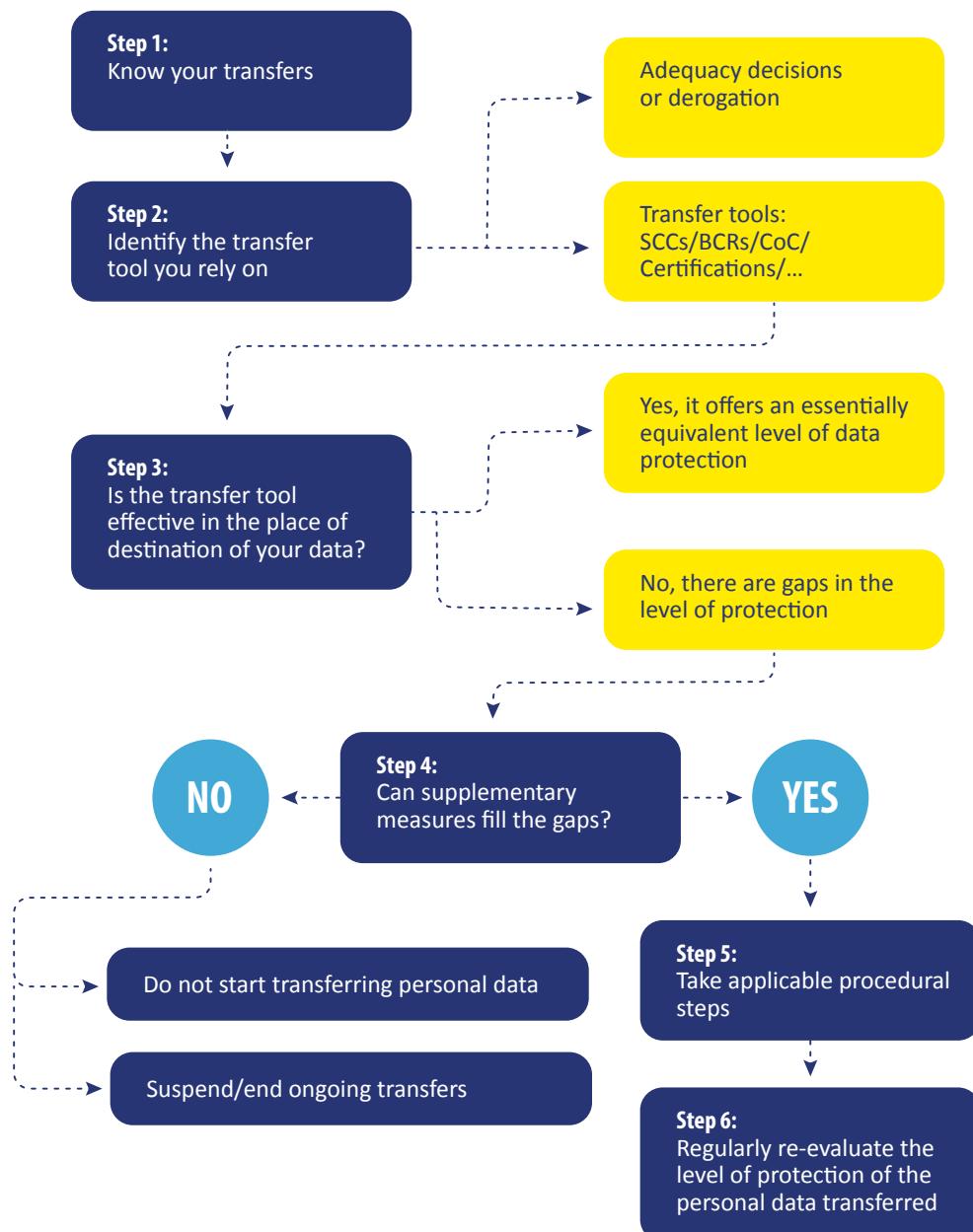
As part of its guidance work following the Case C-311/18 *Schrems II* ruling by the CJEU, the EDPB adopted a final version of its [Recommendations 01/2020](#) following the public consultation that took place at the end of 2020. These aim to help exporters (including controllers, processors, private entities and public bodies) with the complex task of assessing third countries and identifying appropriate supplementary measures where they are needed. Data exporters may need to adopt supplementary measures to ensure that the data they transfer to specific third countries is afforded a level of protection essentially equivalent to that guaranteed in the EU. These recommendations provide data exporters with a series of steps to follow, potential sources of information, and some examples of supplementary measures that could be put in place. The recommendations complement and are consistent with the final version of the European Commission's Standard Contractual Clauses (SCCs) for international data transfers. The EDPB and the European Commission worked together to achieve this. These steps are illustrated below.

#### **3.3.2. EDPS-EDPB Joint Opinion 02/2021 on standard contractual clauses for the transfer of personal data to third countries**

The EDPB and EDPS adopted Joint Opinion 02/2021 on SCCs developed by the European Commission in accordance with Art. 46(1)(c) GDPR relating to the transfer of personal data to third countries. The draft SCCs update and replace the existing

## Roadmap: applying the principle of accountability to data transfers in practice

Roadmap: applying the principle of accountability to data transfers in practice



SCCs for international transfers that were adopted on the basis of Directive 95/46, and take account of the new requirements under the GDPR and the *Schrems II* judgement of the CJEU. Joint Opinion 02/2021 makes clear that the recommendations on supplementary measures are complementary to the SCCs and should therefore guide exporters on how to apply the SCCs correctly. The EDPB also adopted Joint Opinion 01/2021 on standard contractual clauses between controllers and processors under Art. 28(7) GDPR (see Section 5.5.5 for a full summary).

Adopted: 18 June 2021

### 3.4. EDPB-EDPS JOINT OPINION 05/2021 ON THE PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT)

The European Commission presented its Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) on 21 April 2021. AI technologies often involve processing of personal data, so the proposal has important data protection implications. The EDPB and the EDPS adopted Joint Opinion 5/2021. The EDPB and the EDPS raise the following issues:

- **Scope.** The proposal's scope should be expanded so it includes international law enforcement cooperation. Also, it should be clarified in the main text of the proposal that the EU data protection legislation applies to any processing of personal data falling within the scope of the proposal;
- **Risk-based approach and alignment with the GDPR.** The proposal should be aligned with the GDPR when it comes to the concept of "risk to fundamental rights", as well as regarding the rights and remedies available to individuals;

- **Prohibited uses of AI.** Considering high-risk of intrusion into individuals' private lives, great risk of discrimination and effect on human dignity, certain use of AI should be prohibited. In particular, the future regulation should include a general ban on any use of AI for an automated recognition of human features in publicly accessible spaces and should prohibit any type of social scoring. It is also recommended to ban AI systems that categorize individuals from biometrics into clusters, as well as those that infer emotion of natural persons;
- **High-risk AI systems.** External third parties should conduct ex-ante conformity assessments;
- **Governance and European AI Board.** The tasks of the EDPS as the competent authority and the market surveillance authority for the supervision of the Union institutions, agencies and bodies need to be clarified. Data protection authorities should be designated as national supervisory authorities for AI systems considering their expertise and the proposal's close link with the data protection framework. The supervisory authorities for AI systems must be completely independent in the performance of their task in order to guarantee proper supervision and enforcement. The European AI Board (EAIB) should be given more autonomy and powers, moreover, its legal status should be clarified;
- **Regulatory sandboxes and interaction with the data protection framework.** The concept of regulatory sandboxes should be specified, and the EAIB should provide common guidelines on their use. Clarification is needed on compliance mechanisms, particularly on their scope and relationship with other existing measures, such as data protection certifications, seals, marks and codes of conduct.

Adopted: 18 June 2021

### 3.5. BINDING DECISION 01/2021 ON THE DISPUTE ARISEN ON THE DRAFT DECISION OF THE IRISH SUPERVISORY AUTHORITY REGARDING WHATSAPP IRELAND UNDER ART. 65(1)(A) GDPR

The EDPB adopted a binding decision based on Art. 65(1)(a) GDPR which sought to address the lack of consensus on certain aspects of a draft decision issued by the Irish SA as lead supervisory authority (LSA) regarding WhatsApp Ireland Ltd. (WhatsApp IE) and the subsequent objections expressed by a number of concerned supervisory authorities (CSAs). The Irish SA issued the draft decision following an own-volition inquiry into WhatsApp IE, concerning whether WhatsApp IE complied with its transparency obligations pursuant to Arts. 12, 13 and 14 GDPR.

When the Lead Supervisory Authority (LSA) submits a draft decision to the Concerned Supervisory Authorities (CSAs), they may then raise “relevant and reasoned objections” within the set timeframe. Art. 65(1)(a) GDPR requires the EDPB to issue a binding decision when the LSA decides not to follow a relevant and reasoned objection expressed by a CSA or is of the opinion that the objection is not relevant or reasoned. The EDPB sought to clarify the key concepts of this mechanism via two sets of guidelines. First, [Guidelines 09/2020 on relevant and reasoned objection under Regulation 2016/679](#) were adopted in 2020 and finalised after public consultation in March 2021. Second, [Guidelines 03/2021](#) specifically focused on the application of Art. 65(1)(a) GDPR and were adopted in 2021.

In this decision, which was the second instance of application of Art. 65(1)(a) GDPR, after the binding decision adopted in 2020 addressing a dispute concerning the Irish SA’s draft decision on Twitter International Company, the EDPB concluded that the Irish SA should amend its draft decision on WhatsApp IE regarding infringements of transparency, the period to bring processing operations into compliance and the calculation of the fine.

The EDPB analysed the merits of the objections it found to meet the “relevant and reasoned” threshold set by Art. 4(24) GDPR and requested the Irish SA introduce some amendments in its draft decision.

Regarding transparency, the draft decision by the Irish SA already identified a severe breach of Arts. 12 to 14 GDPR. The EDPB identified additional shortcomings with the information provided, affecting users’ ability to understand the legitimate interests being pursued. Therefore, the EDPB requested that the Irish SA to include a finding of an infringement of Art. 13(1)(d) GDPR in [its decision](#). The binding decision also included a request to include a formal finding of an infringement of Art. 13(2)(e) GDPR.

In addition, the EDPB clarified that, while not every infringement of Arts. 12 to 14 GDPR necessarily entails an infringement of Art. 5(1)(a) GDPR, in this particular case, in light of the gravity and the overarching nature and impact of the infringements, there has been an infringement of the transparency principle enshrined in Art. 5(1)(a) GDPR.

Regarding WhatsApp IE’s collection of data of non-users when users decide to use the Contact Feature functionality, the EDPB found that the procedure used by WhatsApp IE did not lead to anonymisation of the collected personal data. Therefore, the EDPB also found that the infringement of Art. 14 GDPR extended to WhatsApp IE’s processing of non-users’ personal data.



Regarding the imposed fine and the calculation of the fine, the EDPB decided that the turnover of an undertaking is not exclusively relevant for the determination of the maximum fine amount in accordance with Art. 83(4)-(6) GDPR, but it may also be considered for the calculation of the fine itself, where appropriate, to ensure the fine is effective, proportionate and dissuasive in accordance with Art. 83(1) GDPR. In this case, the EDPB found the consolidated turnover of the parent company (Facebook Inc.) was to be included in the turnover calculation.

In addition, the EDPB clarified its interpretation of how the calculation of the fine was influenced by the finding of several infringements under Art. 83(3) GDPR. When faced with multiple infringements for the same or linked processing operations, all the infringements should be taken into consideration when calculating the amount of the fine. This is notwithstanding the duty on SAs to take into account the proportionality of the fine and to respect the maximum fine amount set out by the GDPR.

The EDPB also analysed the criteria set by Art. 83(1) and (2) GDPR and concluded that the proposed fine did not adequately reflect the seriousness and severity of the infringements nor did it have a dissuasive effect. Hence, the EDPB instructed the Irish SA to reassess its envisaged fine in accordance with the conclusions reached and impose a higher fine amount.

The Irish SA draft decision included an order to WhatsApp to bring processing operations into compliance within a period of six months. The EDPB found it of primary importance that compliance with transparency obligations was ensured in the shortest timeframe possible. As such, the Irish SA was requested to amend the six-month deadline for compliance to a period of three months.

Adopted: 28 July 2021

### **3.6. URGENT BINDING DECISION 01/2021 ON THE REQUEST UNDER ART. 66(2) GDPR FROM THE HAMBURG (GERMAN) SUPERVISORY AUTHORITY FOR ORDERING THE ADOPTION OF FINAL MEASURES REGARDING FACEBOOK IRELAND LIMITED**

The EDPB adopted its first urgent binding decision under Art. 66(2) GDPR following a request from the Hamburg SA, which had adopted provisional measures against Facebook Ireland Ltd. (Facebook IE) under Art. 66(1) GDPR. The provisional measures prohibited Facebook IE from processing, for 3 months, the data of German residents using WhatsApp for Facebook IE's own purposes, following a change in the Terms of Service and Privacy Policy applicable to European users of WhatsApp IE.

The EDPB decided that the conditions to prove the existence of an infringement to the GDPR and the urgency to adopt final measures were not met, hence stating that the Irish SA did not need to adopt final measures against Facebook IE.

On the issue of an infringement, the EDPB concluded there was a high likelihood that Facebook IE was already processing WhatsApp's user data as a (joint) controller for the common purposes of (i) safety, security and integrity of WhatsApp IE and the other Facebook Companies,<sup>1</sup> and of (ii) improvement of the products of the Facebook Companies. However, due to various contradictions, ambiguities and uncertainties in WhatsApp's user-facing information and written commitments by Facebook IE and WhatsApp IE, the EDPB decided that it was not able to determine with certainty which processing operations are actually being carried out and in which capacity.

Moreover, the EDPB did not have enough information to determine with certainty whether Facebook IE had already started to process WhatsApp's user data as a (joint) controller for its own purposes of marketing communications and

direct marketing, and cooperation with the other Facebook Companies. The EDPB could also not conclude whether Facebook IE had already started or would soon start processing WhatsApp's user data as a (joint) controller for its own purpose in relation to WhatsApp Business API.

On the existence of urgency, the EDPB rejected the Hamburg SA's argument based on Art. 61(8) GDPR as it did not demonstrate that the Irish SA had failed to provide information in the context of a formal request for mutual assistance under Art. 61 GDPR. Besides, the EDPB decided that the adoption of WhatsApp IE's Updated Terms, which contained similar problematic elements as the previous terms, could not, on its own, justify the urgency for the EDPB to order the Irish SA to adopt final measures. Consequently, the EDPB concluded that there was no urgency for the Irish SA to issue final measures against Facebook IE in this case.

However, considering the high likelihood of infringements in particular for the purposes of (i) safety, security and integrity of WhatsApp IE and the other Facebook Companies, and of (ii) improvement of the products of the Facebook Companies, the EDPB requested the Irish SA to perform, as a matter of priority, a statutory investigation. In particular, to show whether Facebook IE was processing WhatsApp user data for such a common purpose of Facebook Companies as a (joint) controller. The Irish SA was requested to verify whether, in practice, Facebook Companies were carrying out processing operations, which implies the combination or comparison of WhatsApp IE's user data with other data sets processed by other Facebook Companies in the context of other apps or services offered by the Facebook Companies, facilitated *inter alia* by the use of unique identifiers. The EDPB asked the Irish SA to determine whether such processing activities were taking place or not and, if they were, whether they had a proper legal basis under Art. 5(1)(a) and Art. 6(1) GDPR.

In addition, taking into consideration the lack of information as regards how personal data are processed for marketing purposes, cooperation with other Facebook Companies and in relation to WhatsApp Business API, the EDPB called upon the Irish SA to further investigate the role of Facebook IE, i.e. whether Facebook IE was acting as a processor or a (joint) controller, with respect to these processing operations.

Adopted: 12 July 2021

<sup>1</sup>. "Facebook Companies" refers to the term as it was defined by WhatsApp in its public-facing information at the time when the EDPB adopted its urgent binding decision (i.e. before the Facebook Group was renamed Meta Group).



# 4



## 2021 - THE EDPB SECRETARIAT

### 4.1. THE EDPB SECRETARIAT

The EDPB Secretariat, which is provided by the European Data Protection Supervisor (EDPS), offers analytical, administrative and logistical support to the EDPB. The EDPB Secretariat is in charge of drafting EDPB documents, providing IT solutions to ensure transparent communications between all the European national Supervisory Authorities (SAs), handling EDPB media relations, as well as organising all EDPB meetings.

A Memorandum of Understanding establishes the terms of cooperation between the EDPB and the EDPS. The staff at the EDPB Secretariat are employed by the EDPS, however, they only work under the instructions of the Chair of the EDPB. At the end of 2021, the staff of the EDPB Secretariat was composed of 31 FTE staff members: one head of the EDPB Secretariat, 6 heads of activity, 12 legal officers, 4

communication officers, 6 administrative assistants and 2 IT officers. The EDPB Secretariat also received the support of three IT external contractors.

The EDPB Secretariat led the drafting of over 35% of the guidelines, opinions, recommendations and statements adopted by the EDPB in 2021 and contributed to a further 25%. In particular, the EDPB Secretariat led the drafting of the Recommendation 01/2020 on the supplementary measures; the EDPB binding decisions (under Art. 65 and Art. 66 GDPR), and the EDPB Strategy and Work Programme.

The EDPB held 389 meetings, including 15 plenary meetings, 200 expert subgroup meetings and 174 drafting team meetings, in comparison to about 100 meetings per year held before the pandemic.

## 4.2. THE EDPB SECRETARIAT'S CONTRIBUTION TO THE NATIONAL SAs' COOPERATION

As part of its 2021-2023 Strategy, the EDPB established a [Support Pool of Experts \(SPE\)](#) in 2020. The terms of reference of the SPE specify that its objectives are to provide material support to the EDPB Members in the form of expertise that is useful for investigations and enforcement activities, and to enhance cooperation and solidarity between the EDPB Members by sharing, reinforcing and complementing strengths and addressing operational needs. In October 2021, a new Head of Activity for Enforcement Support and Coordination was appointed to coordinate the work of the SPE and, in December 2021, EDPB members agreed on SPE priorities for 2022.

Further in line with the 2021-2023 Strategy, the EDPB set up a [Coordinated Enforcement Framework \(CEF\)](#). The CEF provides a structure for recurring annual coordinated action by the SAs. The CEF aims to facilitate joint actions in a flexible and coordinated manner, ranging from joint awareness raising and information gathering to enforcement sweeps and joint investigations. The purpose behind the recurring annual coordinated actions is to promote compliance, empower data subjects to exercise their rights and raise awareness. EDPB members agreed to launch the first coordinated action in 2022 on the use of Cloud based services by the public sector. The EDPB Secretariat is contributing to this work.

The EDPB Secretariat is also in charge of the management of a [register](#) on the EDPB website gathering the final decisions taken concerning cross-border cases in the context of the One-Stop-Shop (OSS) mechanism. The register offers an exceptional opportunity to read final decisions taken by, and involving, different SAs in a cross-border context. These decisions often contain useful guidance on how to comply with the GDPR in practice. The register contains both final decisions and summaries prepared by the EDPB Secretariat

and duly approved by LSAs. See more information under Section 6.1.3 of this Annual Report.

In the context of cooperation between SAs in the assessment of Binding Corporate Rules (BCR) applications, the EDPB Secretariat organised four BCR sessions in 2021. The sessions streamlined discussions between the SAs and the EDPB Secretariat regarding specific aspects of individual BCRs with the aim to facilitate the assessment of the BCRs and work out a consensus on the standards and expectations for BCRs, before the formal procedure is triggered under Art. 64 GDPR. The BCR sessions thus represent a prior informal cooperation phase that aims to address remaining issues that have arisen regarding a specific BCR based on shared comments by the SAs and the EDPB Secretariat.

Additionally, several informal sessions were organised regarding certification criteria. These sessions fostered discussion between the SAs and the EDPB Secretariat on specific certification criteria that may be submitted to the EDPB under Art. 64(1)(c) GDPR.

## 4.3. IT COMMUNICATIONS TOOL (INTERNAL MARKET INFORMATION) AND THE NEW EDPB WEBSITE

With regard to the technical support for SAs' cooperation, throughout 2021, the EDPB Secretariat continued to provide support to the SAs with IT solutions that facilitate their communication. In this respect, the EDPB Secretariat leads the IT Users Expert Subgroup which focuses on assessing the need for development and making changes to the IMI system. Furthermore, it continued to work on best practices to further refine the procedures in use and to share its expertise on the use of the IMI System for the cooperation and consistency mechanism. The EDPB Secretariat also provides an IMI helpdesk to support the staff of the SAs making use of the IMI system. The EDPB IMI helpdesk dealt with 331 requests for support from SAs, and carried out 159 proactive monitoring

procedures to ensure that case files were complete and correctly registered.

The EDPB Secretariat also migrated the EDPB Wiki platform used for internal sharing of information to a new instance dedicated to the EDPB and with an enhanced user experience.

In 2021, the EDPB Secretariat enhanced the EDPB website, '[edpb.europa.eu](http://edpb.europa.eu)', which underwent a new web design.

In the context of functionality, the website now supports dynamic listing of documents and filters, which improves user experience by eliminating numerous general search queries. The communication functionality was improved by providing a new contact form on the website. The content management system of the website, which manages the creation and modification of digital content, was upgraded to Drupal 8. The EDPB Secretariat is also putting great efforts into implementing a new advanced search functionality that will make the website more user-friendly.

### 4.4. THE EDPB SECRETARIAT'S ACTIVITIES RELATING TO ACCESS TO DOCUMENTS

Transparency is a core principle of the EDPB. As an EU body, the EDPB is subject to Art. 15 of the [Treaty of the Functioning of the European Union](#), Regulation 1049/2001 on public access to documents. Art. 76(2) GDPR and Art. 32 of the EDPB's Rules of Procedure reinforce this requirement. The principle of transparency provides any EU citizen, and any natural or legal person residing or having its registered office in a Member State, with the right of access to EDPB documents. This right applies to all documents held by the EDPB, concerning any matter relating to its responsibilities. In exceptional cases, the EDPB may refuse to disclose all or part of a document. The reasons for refusal and other procedural rules are outlined in [Regulation 1049/2001 on public access to documents](#).

In 2021, the EDPB received 39 public access requests for documents held by the EDPB. Confirmatory applications were received in two cases. The EDPB Secretariat is in charge of preparing the answers to those requests, subject to the validation of the EDPB Chair (for confirmatory applications) and Deputy chairs (for initial applications), in accordance with Art. 32(2) of the [EDPB Rules of Procedure](#).

A complaint was made to the European Ombudsman regarding an EDPB confirmatory decision for a request for access to documents, which was submitted in 2020.<sup>2</sup> The request concerned access to some of the preparatory documents for the EDPB Guidelines 02/2019 on the processing of personal data in the context of the provision of online services to data subjects. Following a reassessment of the documents, the EDPB decided to grant partial access to these documents as the fact that differing views expressed in the documents were already publicly known. The complainant was satisfied with the EDPB's reply and the Ombudsman decided to close the case.

<sup>2</sup>. Decision on the EDPB's refusal to grant public access to the preparatory documents for its Guidelines on the processing of personal data in the context of the provision of online services (case 86/2021/AMF).



### 4.5. THE EDPB SECRETARIAT'S ACTIVITIES RELATING TO DATA PROTECTION OFFICER ACTIVITIES

The EDPB processes personal data following Regulation 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 (Regulation 2018/1725). In accordance with Art. 43 of Regulation 2018/1725, the EDPB has designated its own DPO team, which is part of the EDPB Secretariat, to handle the processing of personal data. The DPO's position and tasks are defined in Arts. 44 and 45 of Regulation 2018/1725, and are further detailed in the [EDPB DPO Implementing Rules](#).

In 2021, the EDPB, with the assistance of its DPO team, continued to strengthen the compliance with Regulation 2018/1725 by enhancing its transparency practices through different means, such as:

- The development, publication and update of several privacy notices;
- The continued development of several records, as well as a centralised register for records, which will be made available on the EDPB website;
- The update of its DPO website page with additional information; and
- The improvement of its contact form on the EDPB website.

Furthermore, the DPO team launched several internal legal assessments on various issues concerning the EDPB's processing of personal data and identified suitable legal, organisational and, where applicable, technical solutions. The assessments were also conducted as part of the DPO's advisory role for the EDPB.

In 2021, the DPO team assisted with the handling of six data subject requests under Art. 17 to Art. 24 of Regulation 2018/1725, which indicates a decrease in relation to 2020.

Regarding data breaches, the DPO team assisted with the handling of 12 data breaches under Arts. 34 and 35 of Regulation 2018/1725, which represents an increase in relation to 2020. The assessment of the majority of these data breaches indicated that they were unlikely to result in a risk to the rights and freedoms of natural persons. At the time of the drafting of this report, only one data breach had required a notification to the EDPS.

The DPO team also assisted with several replies to individual requests for information involving the processing of their personal data, including cases where individuals mistakenly assumed that the EDPB processed their personal data.

In addition, the DPO team delivered several internal training sessions and created awareness-raising material, aimed at EDPB Secretariat staff. These activities were tailored to the needs and expertise of the participants to ensure that all staff members, in particular newcomers, were adequately informed of their duties regarding personal data processing, but also of their rights as data subjects.

Finally, the EDPB DPO team continued to liaise closely with other EU institutions, bodies and agencies and their DPOs, particularly in matters involving or related to the processing of personal data, but also to ensure the exchange of good practices, common experiences and tailored approaches to specific data protection challenges. To this end, the DPO team participated in the EU institutions' network of DPOs and the EDPB network of DPOs, comprising the DPOs of national SAs, the EDPS and the EDPB.

# 5



## EUROPEAN DATA PROTECTION BOARD - ACTIVITIES IN 2021

To ensure the consistent application of the GDPR across the EEA, the EDPB issues general guidance to clarify European data protection laws. This guidance provides the public and stakeholders with a consistent interpretation of their rights and obligations, and ensures that national Supervisory Authorities (SAs) have a benchmark for applying and enforcing the GDPR. The EDPB is also empowered to issue opinions or binding decisions to guarantee the consistent application of the GDPR by SAs. Throughout 2021, the EDPB issued multiple guidance and consistency documents, as summarised below.

### 5.1. GENERAL GUIDANCE (GUIDELINES AND RECOMMENDATIONS)

In 2021, the EDPB adopted several guidelines and recommendations on the data protection requirements pertaining to data breach notifications, on codes of conduct as data transfer tools, storing credit card data, virtual voice assistants and the meaning of specific terms in the GDPR. These guidelines and recommendations are summarised below.

## 5.1.1. Guidelines 01/2021 on examples regarding personal data breach notification

The EDPB guidelines aim to help data controllers in deciding how to handle personal data breaches and what factors to consider during risk assessment. Art. 4(12) GDPR defines a “personal data breach” 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”. The practice-oriented, case-based guidance complements the Article 29 Working Party Guidelines on personal data breach notification under Regulation 2016/679, WP 250 and reflects the common experiences of the EEA SAs since the GDPR became applicable.

The guidelines address six categories of personal data breaches and in relation to each of them outline several examples of typical situations based on the SAs’ experiences. The categories of personal data breaches addressed in the guidelines are as follows:

1. **Ransomware attacks** involve malicious code encrypting personal data, where the attacker requires a ransom in exchange for a decryption code.
2. **Data exfiltration attacks** exploit vulnerabilities in services offered over the internet and usually aim to copy, exfiltrate and abuse personal data for some malicious end.
3. **Internal human-related risk source** refers to human errors that lead to personal data breaches, which can have a frequent occurrence and can be both deliberate and accidental, therefore making it difficult for data controllers to identify weaknesses and take steps to avoid them.
4. **Loss or theft of devices and/or documents** is a frequent occurrence of a data breach that might present a difficult risk assessment when devices are no longer available.
5. **Mispostal** involves internal human error due to inattentiveness; there is no malicious action.

6. **Social engineering** refers to attacks involving identity theft and email exfiltration.

For each category of personal data breaches, the guidelines provide advisable, but not exclusive or comprehensive, practical measures and thus provide guidance for dealing with data breaches and future prevention.

Adopted: 14 January 2021 and adopted in its final version following public consultation on 14 December 2021

## 5.1.2. Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive

*See Section 3.2.1 for the full summary.*

The EDPB issued recommendations to provide guidance to the European Commission on the level of data protection in third countries and international organisations under the Law Enforcement Directive (LED). It establishes the core data protection principles that have to be present in a third country’s legal framework or an international organisation to ensure essential equivalence with the EU framework within the scope of the LED. In addition, it may guide third countries and international organisations interested in obtaining adequacy. The finding of an adequate level of data protection does not require a demonstration of a point-by-point mirroring of EU legislation, but rather the effectiveness of the core requirements of legislation in a third country (i.e. enforced and followed in practice).

Adopted: 2 February 2021; formatting changes made on 6 July 2021



### 5.1.3. **Guidance Addendum on certification criteria assessment (Addendum to Guidelines 1/2018 on certification and identifying certification criteria in accordance with Arts. 42 and 43 GDPR)**

The EDPB expanded the framework on certification criteria by adopting this guidance that supplements Guidelines 01/2018 on certification and identifying certification criteria according to Arts. 42 and 43 GDPR (Guidelines 1/2018) and Guidelines 04/2018 on the accreditation of certification bodies under Art. 43 GDPR (2016/679). The improvement of certain aspects of Guidelines 01/2018 aims at assisting stakeholders involved in the drafting of certification criteria in the context of GDPR certification as well as helping SAs and the EDPB in providing consistent evaluation with regard to certification criteria approval.

Scheme owners that intend to submit a certification scheme may be required to commence early informal engagement with the competent SA, which will aid the preparations and clarify the expectations on the scheme.

Controllers or processors may apply for certification of processing activities that involve personal data, however, GDPR certification cannot be provided for standalone products.

All certification schemes shall have a clearly defined scope while indicating what is not permissible, in order to avoid “scope creep”. The scope has to be practical, tractable and provide an added value.

Certification is not about stating an entity is 100% GDPR compliant, but instead aims to show, regarding a concrete Target of Evaluation and its processing operations, that the applicant made everything possible to satisfy certification criteria. The guidance outlines in detail the proper framing of certification criteria and the elements that should be taken into account with regard to certification criteria updates.

Adopted: 6 April 2021 and adopted in its final version following public consultation on 14 December 2021

### 5.1.4. **Guidelines 02/2021 on virtual voice assistants**

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.

A VVA is a service that has the capacity to understand and execute voice requests, as well as to mediate with other IT systems if necessary. Crucial to a VVA's nature is the access and processing of a huge amount of personal data that carries important data protection implications. The EDPB adopted these guidelines in order to advise relevant stakeholders on how to address the most relevant data protection and privacy compliance challenges for VVAs.

The EDPB provides guidance on appropriate legal basis for four of the most common purposes for processing personal data by VVAs: the execution of user requests, the improvement of the VVA machine learning model, biometric identification, and profiling for personalised content or advertising. In this respect, in addition to the GDPR, the [Directive on Privacy and Electronic Communications](#) (ePrivacy Directive) has to be considered. Based on its Art. 5(3), prior consent of a user would be necessary for the storing or gaining of access to information for any purpose other than executing a user's request.

The guidelines also give advice on transparency requirements and recall that, even when it comes to screenless devices, VVA providers must inform users according to the GDPR when setting up the VVA installation or using a VVA app for the first time. All users should also be able to exercise their rights through voice commands. Further, the guidelines

include a list of recommendations on such matters as processing of children's data and sensitive data, as well as on data deletion and data security.

Adopted: 9 March 2021 and adopted in its final version following public consultation on 7 July 2021

## 5.1.5. Guidelines 03/2021 on the application of Art. 65(1)(a) GDPR

Art. 65(1)(a) GDPR is a dispute resolution mechanism provided by the EDPB in case of dispute between SAs relating to the enforcement activities in the framework of a One-Stop-Shop (OSS) procedure. It is designed to guarantee the GDPR's correct and consistent application in circumstances involving cross-border processing of personal data.

This mechanism aims at settling conflicting views arising on the merits of a case between the Lead Supervisory Authority (LSA) and Concerned Supervisory Authorities (CSAs) who have lodged relevant and reasoned objections on a draft decision.

The EDPB elaborates on the application of relevant provisions of the GDPR and the EDPB Rules of Procedure, lays out an outline of the main stages of the procedure and clarifies its competence when adopting a legally binding decision under Art. 65(1)(a) GDPR. The guidelines also include an overview of the applicable procedural safeguards (such as the right to be heard, access to the file and the duty to give reasons).

Adopted: 13 April 2021

## 5.1.6. Recommendations 02/2021 on the legal basis for the storage of credit card data for the sole purpose of facilitating further online transactions

The continuous development of the digital economy and e-commerce has increased the number of online transactions.

This increase heightens the risk of fraud associated with the use of credit card data online. Against this background, the EDPB has issued recommendations clarifying the legal basis for the storage of credit card data by online providers of goods and services, for the sole and specific purpose of facilitating further purchases by data subjects. These recommendations cover situations in which data subjects buy a product or pay for a service via a website or an application and provide their credit card data in order to conclude a unique transaction.

In such situations, consent (Art. 6(1)(a) GDPR) appears to be the sole appropriate legal basis for storing credit card data for future purchases. The controller should ensure that the data subject provides GDPR-standard consent to store the credit card data after a purchase. The consent must be freely given, specific, informed and unambiguous. It must be delivered by a clear affirmative action and should be requested in a user-friendly way, such as through a checkbox that is not pre-ticked. Additionally, it must be distinguished from the consent given for terms of service or sales and it cannot be a condition to the completion of a transaction.

In accordance with Art. 7(3) GDPR, data subjects have the right to withdraw their consent for the storing of credit card data for the purposes of facilitating further purchases at any time. Such withdrawal must be free, simple and as easy for the data subject as it was to give consent. As a consequence of a withdrawal, the controller must effectively delete the credit card data stored for the sole purpose of facilitating further online transactions.

Adopted: 19 May 2021

## 5.1.7. Guidelines 04/2021 on codes of conduct as tools for transfers

The EDPB expanded the general framework for the adoption of codes of conduct (CoCs) provided under [Guidelines 1/2019](#)

on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 by adopting these complementary guidelines. Their main purpose is to specify the application of Art. 40(3) and Art. 46(2)(e) GDPR relating to CoCs as appropriate safeguards for transfers of personal data to third countries. These GDPR provisions stipulate that a valid CoC may also be adhered to and used by controllers and processors not subject to the GDPR to provide appropriate safeguards for transfers of personal data outside of the EEA.

The CoC must be accompanied by a legally binding instrument, whereby the data importer commits to comply with the obligations set forth in the CoC, in order to ensure that the transferred personal data remains adequately protected, as per GDPR standards, when transferred outside the EEA. From a content perspective, the CoC should provide appropriate safeguards that include (1) essential principles, rights and obligations under the GDPR and (2) guarantees specific to the context of the transfer.

The guidelines include a checklist of minimum elements that a transfer CoC should include, which, depending on the transfer scenario, may need to be supplemented with additional commitments and measures.

In terms of the adoption process, the parties submitting a transfer CoC for approval must obtain the approval decision of the CSA following a favourable opinion from the EDPB and an implementing decision by the European Commission giving general validity to the CoC.

Adopted: 7 July 2021



### **5.1.8. Guidelines 05/2021 on the Interplay between the application of Art. 3 and the provisions on international transfers as per Chapter V of the GDPR**

To clarify the interplay between the territorial scope of Art. 3 GDPR and the provisions on international transfers in Chapter V of the GDPR, the EDPB's guidance provides a consistent interpretation of the concept of international transfers. It aims to assist controllers and processors with identifying whether a processing operation constitutes an international transfer.

There are three cumulative criteria that must be met for data processing to be classified as a transfer:

1. A controller or processor ("exporter") is subject to the GDPR for the given processing;
2. This controller or processor transmits or makes available the personal data to another controller, joint controller or processor; and
3. This other controller, joint controller or processor is in a third country or is an international organisation ("data importer"), irrespective of whether or not the importer is already subject to the GDPR under Art. 3 GDPR.

The EDPB clarifies that disclosure of data made directly available by individuals and on their own initiative, are not transfers as there is no data exporter, meaning a controller or processor sending the data abroad.

If the identified criteria are not met, there is no transfer and Chapter V of the GDPR does not apply.

Adopted: 18 November 2021

## 5.1.9. Guidelines adopted after public consultation

### 5.1.9.1. Guidelines 09/2020 on relevant and reasoned objection under Regulation 2016/679

To clarify the OSS cooperation mechanism for SAs outlined in the GDPR, the EDPB guidance establishes a common understanding of the notion of a “relevant and reasoned” objection, on the basis of the definition enshrined in Art. 4(24) GDPR, and addresses its interpretation.

Under the OSS cooperation mechanism, and specifically under Art. 60(3) and (4) GDPR, an LSA is required to submit a draft decision to the CSAs, who may then raise a “relevant and reasoned objection” within a set timeframe. In this context, the EDPB further clarifies the meaning of each of the elements of the definition in Art. 4(24) GDPR.

The guidelines explain that in order for an objection to be “relevant”, there should be a direct connection between the substance of the draft decision at hand and the objection, since the objection, if followed, would entail a change to the draft decision leading to a different conclusion. The EDPB further clarifies that the objection needs to concern either whether there is an infringement of the GDPR or whether the envisaged action towards the controller or processor complies with the GDPR.

The objection will be adequately “reasoned” when it is clear, precise, coherent and detailed in explaining the reasons for objection, through legal or factual arguments. The EDPB also provides clarification on the obligation for the CSAs to clearly demonstrate in their objection the significance of the risks posed by the draft decision for the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data.

The first version of the guidelines was adopted on 8 October 2020 and updates were included in the guidelines in 2021 following the public consultation.

Adopted: 9 March 2021

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

As they move into our everyday lives, connected vehicles have become a significant subject for regulators, particularly as they require personal data processing within a complex ecosystem.

The guidelines focus on the processing of personal data in relation to the non-professional use of connected vehicles. They clarify key privacy and data protection risks, including the security of personal data, ensuring full control over the processing, the appropriate legal basis for the processing and how GDPR-compliant consent should be collected.

To help controllers mitigate the risks for data subjects, the EDPB identifies three categories of personal data requiring special attention:

1. **Location data**, which has a particularly sensitive nature, due to it possibly revealing life habits;
2. **Biometric data**, for which special protection is provided in Art. 9 GDPR;
3. **Data revealing criminal offences** and other infractions, whose processing is subject to the safeguards contained in Art. 10 GDPR.

The EDPB also highlights the interplay between the GDPR and the ePrivacy Directive, noting that the connected vehicle and any device connected to it should be considered “terminal equipment” for the purposes of Art. 5(3) of the ePrivacy Directive. It further outlines the considerations to be taken for a lawful processing under the two instruments.

Lastly, the EDPB presents multiple case studies, such as “pay as you drive” insurance schemes, automatic emergency calls and accidentology studies.

The first version of the guidelines was adopted on 28 January 2020 and updates were included in the guidelines in 2021 following the public consultation.

Adopted: 9 March 2021

### 5.1.9.3. Guidelines 08/2020 on the targeting of social media users

As mechanisms used to target social media users become more sophisticated and an increasingly large number of data sources are combined and analysed for targeting purposes, the topic has gained increased public interest and regulatory scrutiny.

Within this environment, the EDPB identifies three key actors:

- 1. Users:** individuals who make use of social media;
- 2. Social media providers:** providers of an online service that enables the development of networks of users;
- 3. Targeters:** natural or legal persons that use social media services to direct specific messages to users.

Referring to relevant caselaw of the CJEU, such as the judgments in Case C-40/17 (*Fashion ID*), Case C-25/17 (*Jehovah’s Witnesses*) and Case C-210/16 (*Wirtschaftsakademie*), the EDPB provides specific examples to clarify the roles of targeters and social media providers within different targeting

mechanisms. Social media providers and targeters are often identified as joint controllers for the purposes of Art. 26 GDPR.

When it comes to targeting social media users, they may be targeted on the basis of provided, observed or inferred data, as well as a combination thereof.

There are numerous risks posed to the rights and freedoms of individuals as a result of processing personal data, including the possibility of discrimination and exclusion, and the potential for manipulating and influencing users. In this context, the EDPB highlights the relevant transparency requirements, the right of access and the joint controllers’ duty to conduct a Data Protection Impact Assessment if the processing operations are “likely to result in a high risk” to the rights and freedoms of data subjects.

The first version of the guidelines was adopted on 2 September 2020 and updates were included in the guidelines in 2021 following the public consultation.

Adopted: 13 April 2021



### 5.1.9.4. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

In its judgment in [Case C-311/18 \(Schrems II\)](#), the CJEU reaffirmed that the protection granted to personal data in the EEA must travel with the data wherever it goes. The level of protection in third countries does not need to be identical to that guaranteed within the EEA, but essentially equivalent. According to the CJEU, data exporters may implement supplementary measures to fill gaps in protection and bring it up to the level required by EU law, where Art. 46 GDPR transfer tools cannot guarantee it by themselves. The EDPB issued recommendations on 10 November 2020 that provide data exporters with a series of six steps to follow to apply the principle of accountability to data transfers, and some examples of supplementary measures. Updates were included in the guidelines in 2021 following the public consultation.

Adopted: 18 June 2021

### 5.1.9.5. Guidelines 07/2020 on the concepts of controller and processor in the GDPR

This updated EDPB guidance builds upon and replaces the Article 29 Working Party [Opinion 01/2010 on the concepts of “controller” and “processor”](#) (WP169). The correct interpretation of the concepts of controller, joint controller and processor have been crucial in the application of the GDPR, since these actors determine who shall be responsible for compliance with different data protection rules, and how data subjects can exercise their rights in practice.

Following the public consultation, the EDPB further elaborated upon its guidance, adding clarifications on, amongst others, the distinction between essential and non-essential means, issues concerning joint controllership and processors' roles in relation to data breaches.

The first version of the guidelines was adopted on 2 September 2020 and updates were included in the guidelines in 2021 following the public consultation.

Adopted: 7 July 2021

### 5.1.9.6. Guidelines 10/2020 on restrictions under Art. 23 GDPR

The GDPR allows for data subject rights to be restricted in exceptional circumstances. The EDPB adopted the final version of its guidance with regards to restrictions of data subject rights under Art. 23 GDPR. The guidelines recall the conditions surrounding the use of such restrictions in light of the EU Charter of Fundamental Rights and the GDPR. They provide a thorough analysis of the criteria to apply restrictions, the assessments that must be observed, how data subjects can exercise their rights after the restrictions are lifted, and the consequences of infringing Art. 23 GDPR.

The first version of the guidelines was adopted on 15 December 2020 and updates were included in the guidelines in 2021 following the public consultation.

Adopted: 13 October 2021

## 5.2. CONSISTENCY OPINIONS

### 5.2.1. Opinions on draft decisions regarding Binding Corporate Rules

SAs may approve Binding Corporate Rules (BCRs) within the meaning of Art. 47 GDPR. BCRs are data protection policies implemented and adhered to within a group of enterprises established in the EEA for transfers of personal data outside the EEA within the same group. In 2021, several SAs submitted their draft decisions regarding the controller or processor

BCRs of various companies to the EDPB, requesting an opinion under Art. 64(1)(f) GDPR. The EDPB issued eighteen opinions on BCRs.

In all instances, the EDPB concluded that the draft BCRs contained all required elements and guaranteed appropriate safeguards to ensure that the level of protection guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. It is without prejudice to the obligation of the data exporter to assess whether, in the specific case, additional measures are necessary in order to ensure an essentially equivalent level of protection as provided in the EU. In any case, on the basis of the EDPB opinions, the BCRs could be approved without changes by the relevant SAs.

The various opinions are listed below:

- Opinion 01/2021 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of Saxo Bank Group Adopted: 22 January 2021
- Opinion 02/2021 on the draft decision of the Swedish Supervisory Authority regarding the Controller Binding Corporate Rules of Elanders Group Adopted: 22 January 2021
- Opinion 03/2021 on the draft decision of the Belgian Supervisory Authority regarding the Controller Binding Corporate Rules of BDO Adopted: 22 January 2021
- Opinion 04/2021 on the draft decision of the Belgian Supervisory Authority regarding the Processor Binding Corporate Rules of BDO Adopted: 22 January 2021
- Opinion 06/2021 on the draft decision of the Spanish Supervisory Authority regarding the Processor Binding Corporate Rules of Kumon Group Adopted: 16 February 2021
- Opinion 07/2021 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of Kumon Group Adopted: 16 February 2021
- Opinion 08/2021 on the draft decision of the Baden-Wurttemberg Supervisory Authority regarding the Processor Binding Corporate Rules of Luxoft Group Adopted: 16 February 2021
- Opinion 09/2021 on the draft decision of the Baden-Wurttemberg Supervisory Authority regarding the Controller Binding Corporate Rules of Luxoft Group Adopted: 16 February 2021
- Opinion 21/2021 on the draft decision of the French Supervisory Authority regarding the Controller Binding Corporate Rules of the CGI Group Adopted: 1 July 2021
- Opinion 22/2021 on the draft decision of the French Supervisory Authority regarding the Processor Binding Corporate Rules of the CGI Group Adopted: 1 July 2021
- Opinion 26/2021 on the draft decision of the Supervisory Authority of North Rhine-Westphalia (Germany) regarding the Controller Binding Corporate Rules of the Internet Initiative Japan Group Adopted: 2 August 2021
- Opinion 27/2021 on the draft decision of the Supervisory Authority of North Rhine-Westphalia (Germany) regarding the Processor Binding Corporate Rules of the Internet Initiative Japan Group Adopted: 2 August 2021
- Opinion 28/2021 on the draft decision of the Belgian Supervisory Authority regarding the Controller Binding Corporate Rules of Oregon Tool, Inc (formerly "Blount") Adopted: 2 August 2021
- Opinion 29/2021 on the draft decision of the Belgian Supervisory Authority regarding the Processor Binding Corporate Rules of Oregon Tool, Inc (Formerly "Blount") Adopted: 2 August 2021
- Opinion 30/2021 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of Oregon Tool, Inc (Formerly "Blount") Adopted: 2 August 2021

Supervisory Authority regarding the Processor Binding Corporate Rules of the COLT Group Adopted: 2 August 2021

- Opinion 31/2021 on the draft decision of the Spanish Supervisory Authority regarding the Processor Binding Corporate Rules of the COLT Group Adopted: 2 August 2021
- Opinion 33/2021 on the draft decision of the Belgian Supervisory Authority regarding the Controller Binding Corporate Rules of Carrier Adopted: 26 October 2021
- Opinion 34/2021 on the draft decision of the Belgian Supervisory Authority regarding the Controller Binding Corporate Rules of Otis Adopted: 26 October 2021

## 5.2.2. Opinions on draft requirements for accreditation of a certification body

Seven SAs submitted their draft decisions on accreditation requirements for certification bodies under Art. 43(1)(b) GDPR to the EDPB, requesting an opinion under Art. 64(1)(c) GDPR.

These requirements allow the accreditation of certification bodies responsible for issuing and renewing certification in accordance with Art. 42 GDPR.

These opinions aim to establish a consistent and harmonised approach regarding the requirements that SAs and national accreditation bodies apply when accrediting certification bodies under the GDPR. To do so, the EDPB made several recommendations and encouragements to the relevant SAs on the amendments to be made to the draft accreditation requirements.

The SAs then amended their drafts in accordance with Art. 64(7) GDPR, taking utmost account of the opinions of the EDPB.

The various opinions are listed below:

- Opinion 12/2021 on the draft decision of the competent Supervisory Authority of Portugal regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR Adopted: 20 July 2021
- Opinion 13/2021 on the draft decision of the competent Supervisory Authority of Romania regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR Adopted: 23 March 2021
- Opinion 19/2021 on the draft decision of the competent Supervisory Authority of Hungary regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR Adopted: 1 June 2021
- Opinion 25/2021 on the draft decision of the competent Supervisory Authority of Lithuania regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR Adopted: 20 July 2021
- Opinion 35/2021 on the draft decision of the competent Supervisory Authority of Belgium regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR Adopted 30 November 2021
- Opinion 36/2021 on the draft decision of the competent Supervisory Authority of Norway regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR Adopted 30 November 2021
- Opinion 38/2021 on the draft decision of the competent Supervisory Authority of Latvia regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR Adopted 20 November 2021



### 5.2.3. Opinions on SAs' approval of accreditation requirements for code of conduct monitoring body

The EDPB issued five opinions on draft accreditation requirements for code of conduct monitoring bodies, as requested by the submitting SAs in accordance with Art. 64(1) (c) GDPR.

The aim of such EDPB opinions is to ensure consistency and the correct application of the requirements among EEA SAs. To do so, the EDPB made several recommendations and encouragements to the various SAs on the amendments to be made to the draft accreditation requirements. On this basis, the SAs amended their drafts in accordance with Art. 64(7) GDPR, taking utmost account of the opinions of the EDPB.

The various opinions are listed below:

- Opinion 10/2021 on the draft decision of the competent Supervisory Authority of Hungary regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted: 23 March 2021
- Opinion 11/2021 on the draft decision of the competent Supervisory Authority of Norway regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted: 23 March 2021
- Opinion 23/2021 on the draft decision of the competent Supervisory Authority of Czech Republic regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted: 20 July 2021

- Opinion 24/2021 on the draft decision of the competent Supervisory Authority of Slovakia regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted: 20 July 2021
- Opinion 37/2021 on the draft decision of the competent Supervisory Authority of Malta regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted 30 November 2021

### 5.2.4. Opinion on SAs' draft Standard Contractual Clauses

Opinion 18/2021 on the draft Standard Contractual Clauses submitted by the LT SA (Art. 28(8) GDPR)

The contract or other legal act to govern the relationship between the controller and the processor in accordance with Art. 28(3) GDPR may be based, in whole or in part, on Standard Contractual Clauses (SCCs).

An SA may adopt SCCs in accordance with the consistency mechanism. As such, the EDPB reviews draft SCCs submitted by SAs to contribute to the consistent application of the GDPR throughout the EEA. In March 2021, the Lithuanian SA (LT SA) submitted its draft SCCs to the EDPB, requesting an opinion under Art. 64(1)(d) GDPR. The EDPB held that the draft SCCs needed some further adjustments and proposed several recommendations and encouragements on how to amend them.

Adopted: 19 May 2021



### 5.2.5. Opinions on SAs' approval of codes of conduct

Two SAs submitted their draft decisions on the approval of two codes of conduct that related to processing activities in several Member States. The codes of conduct were reviewed in accordance with the procedures set up by the EDPB in Guidelines 04/2021 on codes of conduct and in the EDPB Document on the procedure for the development of informal "Codes of Conduct sessions". Those codes of conduct do not aim to be used as a tool for international transfer of data (Art. 46(2)(e) GDPR).

The EDPB considered that the draft codes complied with the GDPR as they fulfilled the requirements imposed by Art. 40 and Art. 41 GDPR. The EDPB also recalled that, in accordance with Art. 40(5) GDPR, the competent SA would have to submit the code of conduct to the EDPB in case of amendment or extension.

The various opinions are listed below:

- Opinion 16/2021 on the draft decision of the Belgian Supervisory Authority regarding the "EU Data Protection Code of Conduct for Cloud Service Providers" submitted by Scope Europe Adopted: 19 May 2021
- Opinion 17/2021 on the draft decision of the French Supervisory Authority regarding the European code of conduct submitted by the Cloud Infrastructure Service Providers (CISPE) Adopted: 19 May 2021

### 5.2.6. Opinion on SAs' authorisation of administrative arrangements

Opinion 05/2021 on the draft Administrative Arrangement for the transfer of personal data between the Haut Conseil du Commissariat aux Comptes (H3C) and the Public Company Accounting Oversight Board (PCAOB)

The Haut Conseil du Commissariat aux Comptes submitted a draft Administrative Arrangement for the transfers of personal data between the Haut Conseil du Commissariat aux Comptes and the Public Company Accounting Oversight Board to the French SA, which thereafter requested an opinion from the EDPB pursuant to Art. 64(2) GDPR.

The EDPB welcomed the efforts made for this Administrative Agreement, which included a number of important data protection safeguards in line with the GDPR as well as with the safeguards laid down in EDPB Guidelines 02/2020, and underlined some key considerations.

Adopted: 2 February 2021

### 5.2.7. Opinion on the legal basis for an SA to order ex officio data erasure

Opinion 39/2021 on whether Art. 58(2)(g) GDPR could serve as a legal basis for a supervisory authority to order ex officio the erasure of personal data, in a situation where such request was not submitted by the data subject.

The Hungarian SA requested the EDPB to issue an opinion on whether Art. 58(2)(g) GDPR could serve as a legal basis for an SA to order ex officio the erasure of unlawfully processed personal data, in a situation where such a request was not submitted by the data subject. The EDPB concluded that Art. 58(2)(g) was a valid legal basis in such a situation.

Adopted: 14 December 2021



## **5.3. BINDING DECISIONS**

### **5.3.1. Binding Decision 01/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Art. 65(1)(a) GDPR**

*See Section 3.5 for a full summary.*

In relation to the draft decision regarding WhatsApp Ireland (WhatsApp IE) of the Irish SA and the subsequent CSA objections, the EDPB adopted a binding decision under Art. 65(1)(a) GDPR. The decision concludes that the Irish SA should amend its draft decision regarding infringements of transparency, the period to bring processing operations into compliance and the calculation of the fine.

Adopted: 28 July 2021

### **5.3.2. Urgent Binding Decision 01/2021 on the request under Art. 66(2) GDPR from the Hamburg (German) Supervisory Authority for ordering the adoption of final measures regarding Facebook Ireland Limited**

*See Section 3.6 for a full summary.*

Following a request from the Hamburg SA, which had taken provisional measures, in accordance with Art. 66(1) GDPR, against Facebook Ireland Ltd. (Facebook IE) banning their processing of WhatsApp IE user data in Germany for their own purposes, the EDPB adopted an urgent binding decision under Art. 66(2) GDPR.

The decision states that the conditions to prove the existence of an infringement and urgency were not met. The decision concludes that there is a high likelihood that Facebook IE already processes WhatsApp IE user data as a (joint) controller for a number of purposes, which could not be demonstrated

with certainty due to contradictions, ambiguities and uncertainties noted in the evidence provided. Due to the high likelihood of infringements of the GDPR, the decision requests the Irish SA to carry out, as a matter of priority, a statutory investigation to determine whether such processing activities are taking place or not, and if it is the case, whether they have a proper legal basis under GDPR.

Adopted: 12 July 2021

## **5.4. REGISTER FOR DECISIONS TAKEN BY SUPERVISORY AUTHORITIES AND COURTS ON ISSUES HANDLED IN THE CONSISTENCY MECHANISM**

The EDPB maintains a publicly accessible electronic [register of decisions](#) taken by SAs and courts on issues handled in the consistency mechanism per Art. 70(1)(y) GDPR. This register provides for accessibility and transparency of the decisions and further promotes the consistent application of the GDPR by the European SAs.

All the decisions added in 2021 are related to decisions made by the SAs following the EDPB consistency opinions or following the 01/2021 EDPB binding decision regarding a dispute on an Irish SA draft decision on WhatsApp.

[See Section 5.2](#) on consistency opinions and [Section 5.3](#) on binding decisions.



## **5.5. LEGISLATIVE CONSULTATION AND DOCUMENTS ADDRESSED TO THE EUIS OR NATIONAL AUTHORITIES**

### **5.5.1. Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom**

*See Section 3.2.2 for a full summary.*

When providing an assessment of the draft implementing decision on the adequacy of personal data protection offered by the UK under the GDPR, the EDPB finds that, as the UK is a former EU Member State, many aspects of the UK's data protection framework are essentially equivalent to those in the EU. However, there are several potential challenges with essential equivalence of UK and EU data protection law and the European Commission should monitor future developments.

### **5.5.2. Opinion 15/2021 regarding the European Commission Draft Implementing Decision pursuant to Directive (EU) 2016/680 on the adequate protection of personal data in the United Kingdom**

*See Section 3.2.3 for a full summary.*

The EDPB recognises that many aspects of UK's data protection framework are essentially equivalent to the protections offered in the EU. Mindful of the possibility that the UK deviates in the future from the EU data protection framework, the EDPB welcomes the addition of a sunset clause into the draft decision. In addition, it further emphasises the importance of the European Commission in monitoring the developments of UK's data protection framework and, if after the adoption of

the adequacy decision the adequate level of protection is no longer ensured, in taking actions by suspending, amending or repealing the adequacy decision.

### **5.5.3. Opinion 20/2021 on Tobacco Traceability System**

On 3 March 2021, the European Commission requested the opinion of the EDPB, on the basis of Art. 70(1)(b) GDPR, on three questions related to the different roles of the actors involved in the tobacco traceability system established under Directive 2014/40/EU.

- First, the European Commission asked the EDPB whether it agrees with the European Commission's assessment according to which the Member States and the European Commission act as joint controllers with regard to the processing of personal data in the context of the EU tobacco traceability system. The EDPB considers that the European Commission has taken into consideration the necessary elements to perform the assessment of joint controllership. To achieve the purpose of monitoring compliance with and enforcing the rules, all the means identified (i.e. the ID Issuers' registries and the repositories) were necessary, since otherwise the traceability of tobacco products would not be possible and thus the purpose of processing would not be achievable.



- Second, the European Commission asked whether the EDPB agrees with the European Commission's assessment according to which the ID Issuers act as processors of the Member States. In response, the EDPB holds that the European Commission has not taken into consideration all the necessary elements to perform the assessment on the role of the ID Issuers. In this regard, it should be noted that, in case of joint controllership, the mere fact that the ID Issuers are appointed by the Member State, does not necessarily imply that they are only processors of the Member State.
- Third, the European Commission asked whether the EDPB agrees with the European Commission's assessment according to which the independent third parties hosting the primary repositories act as sub-processors of the operator of the secondary repository acting as a processor on behalf of the joint controllers (European Commission and the Member States). The EDPB states that the European Commission has taken into consideration the necessary elements to perform the assessment on the role of the providers of the primary repository.

The EDPB considerations regarding the European Commission's questions are without prejudice to any specific further assessment pursuant to applicable data protection legislation carried out by the controller as part of its obligations or by a competent SA in the exercise of its powers.

Adopted: 18 June 2021



### 5.5.4. **Opinion 32/2021 regarding the European Commission draft implementing decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the Republic of Korea**

On 16 June 2021, the European Commission launched the formal process towards the adoption of its draft implementing decision on the adequate protection of personal data in the Republic of Korea under the Personal Information Protection Act pursuant to Art. 45 GDPR.

On the same date, the European Commission asked for the opinion of the EDPB in accordance with Art. 70(1)(s) GDPR. The EDPB assessed the level of protection afforded in the Republic of Korea on the basis of the draft decision itself, as well as on the documentation made available by the European Commission.

The EDPB assessed both the general GDPR aspects of the draft decision and the access by public authorities to personal data transferred from the EEA for the purposes of law enforcement and national security, including the legal remedies available to individuals in the EEA. The EDPB also assessed whether the safeguards provided under the South Korean legal framework are in place and effective.

The EDPB recognises that key aspects of South Korea's data protection framework are essentially equivalent to the protections offered in the EU, and welcomes the notifications adopted by the South Korean data protection authority, which provide relevant clarifications on some important safeguards considered within the adequacy assessment. The EDPB identifies some aspects to be further clarified and closely monitored by the European Commission.

Adopted: 24 September 2021

### 5.5.5. EDPB-EDPS Joint Opinion 01/2021 on standard contractual clauses between controllers and processors

On 12 November 2020, the European Commission published a draft Implementing Decision on Standard Contractual Clauses (SCCs) between controllers and processors for the matters referred to in Art. 28(3) and (4) GDPR and Art. 29(7) of Regulation (EU) 2018/1725 as well as a draft Annex containing the draft SCCs.

The European Commission requested a joint opinion of the EDPB and the EDPS on the basis of Art. 42(1) and (2) of Regulation (EU) 2018/1725 on this set of draft SCCs.

The joint opinion aims at ensuring consistency and a correct application of Art. 28 GDPR as regards the presented draft clauses that could serve as SCCs in compliance with Art. 28(7) GDPR and Art. 29(7) of Regulation (EU) 2018/1725.

The joint opinion comprises (i) a core part detailing general comments made by the EDPB and the EDPS and (ii) an annex where comments of a more technical nature were made directly to the Draft Decision and the Draft SCCs to provide some examples of possible amendments with the aim of bringing more clarity to the text and ensuring its practical usefulness in day-to-day operations of controllers and processors. The EDPB and the EDPS commented, inter alia, on the interplay with the other set of European Commission draft SCCs on transfers (see Section 5.5.6 below), the so-called “docking clause”, which allows additional entities to accede to the SCCs, and other aspects relating to obligations for processors. Additionally, the EDPB and EDPS suggest that the Annexes to the SCCs clarify as much as possible the roles and responsibilities of each of the parties with regard to each processing activity.

Adopted: 14 January 2021

### 5.5.6. EDPB-EDPS Joint Opinion 02/2021 on standard contractual clauses for the transfer of personal data to third countries

On 12 November 2020, the European Commission requested the EDPB and the EDPS to issue a joint opinion on its draft implementing decision on SCCs for the transfer of personal data to third countries (joint opinion), in compliance with Art. 42(2) of Regulation (EU) 2018/1725. These draft SCCs aimed at updating and replacing the previous sets of SCCs adopted by the European Commission based on Directive 95/46/EC.

The joint opinion comprises (i) a core part detailing general comments and (ii) an annex with additional comments of a more technical nature made directly to the draft SCCs to provide some examples of possible amendments.

Overall, the EDPB and the EDPS note with satisfaction that the draft SCCs present a reinforced level of protection for data subjects, in particular, the specific provisions intending to address some of the main issues identified in the CJEU ruling in Case C-311/18 (Schrems II) and to reflect several measures identified in EDPB Recommendations 01/2020 on supplementary measures.

The EDPB and the EDPS also welcome the fact that this draft brings the previous SCCs in line with new GDPR requirements, and better reflects the widespread use of new and more complex processing operations often involving multiple data importers and data exporters, long and complex processing chains, as well as evolving business relationships.



The EDPB and EDPS consider that several provisions of the draft SCCs could be improved or clarified, such as the scope of the SCCs, certain third-party beneficiary rights, certain obligations regarding onward transfers, aspects of the assessment of third country laws regarding access to public data by public authorities, and the notification to the SA.

Adopted: 14 January 2021

### **5.5.7. EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act)**

On 25 November 2020, the European Commission requested a joint opinion of the EDPB and the EDPS, on the basis of Article 42(2) of Regulation (EU) 2018/1725, on the Proposal for the Data Governance Act (the Proposal).

The EDPB and the EDPS highlight that the Proposal is of particular importance for the protection of individuals' rights and freedoms with regard to the processing of personal data. The scope of the opinion is limited to aspects of the Proposal related to the protection of personal data, which, as observed, represents a key - if not the most important - aspect of the Proposal.

The EDPB and the EDPS point out inconsistencies with the EU data protection legislation (as well as with other EU legislation, such as the Open Data Directive) and problems of the Proposal, which raises a significant number of serious concerns, often intertwined, related to the protection of the fundamental right to the protection of personal data. The EDPB and the EDPS provide advice and recommendations to the co-legislators to ensure in particular: legal certainty for natural persons, economic operators and public authorities; due protection of personal data for data subjects in line with the Treaty on the Functioning of the EU (TFEU), the EU Charter

of Fundamental Rights and the data protection acquis; and a sustainable digital environment including the necessary "checks and balances".

Overall, the EDPB and the EDPS note that the Proposal, also having regard to the Impact Assessment accompanying it, does not duly take into account the need to ensure and guarantee the level of protection of personal data provided under EU law. The EDPB and the EDPS consider that this policy trend toward a data-driven economy framework without sufficient consideration of personal data protection aspects raises serious concerns from a fundamental rights viewpoint.

The EDPB and the EDPS furthermore highlight that the European Union model relies on the mainstreaming of its values and fundamental rights within its policy developments, and that the GDPR must be considered as a foundation on which to build a European data governance model. The EU legal framework in the field of personal data protection shall be considered as an enabler, rather than an obstacle, to the development of a data economy that corresponds to the Union values and principles.

Adopted: 10 March 2021

### **5.5.8. EDPB-EDPS Joint Opinion 04/2021 on the Proposal for a Regulation of the European Parliament and of the Council on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery to facilitate free movement during the COVID 19 pandemic (Digital Green Certificate)**

The EDPB and the EDPS note that the Proposal for a Regulation concerning the Digital Green Certificate aims at facilitating the exercise of the right to free movement within the EU during the COVID-19 pandemic by establishing a common framework, thus requiring all EU Member States to use the

Digital Green Certificate framework and issue certificates for that purpose.

The EDPB and the EDPS consider it essential to ensure that the Proposal is consistent and does not conflict in any manner with the application of the GDPR. Compliance with the principles of necessity and proportionality by the measures introduced with the Proposal should be carefully analysed. In this regard, the EDPB and EDPS underline the lack of an impact assessment accompanying the Proposal, which would provide substantiation of the impact of the measures and the effectiveness of already existing, less intrusive measures. They also underline that the Proposal must not lead to the creation of any sort of personal data central database at EU level under the pretext of the establishment of the Digital Green Certificate framework. Furthermore, the joint opinion includes specific comments about the categories of personal data, the adoption of adequate technical and organisational privacy and security measures, the identification of controllers and processors, the transparency and data subject's rights, the data storage and the international data transfers.

The Proposed Regulation did not address the use of the Digital Green Certificate framework at national level for other reasons than facilitating the free movement between EU Member States. In this regard, the Proposal may not be used as a legal basis for such further use. The EDPB and the EDPS also remark that any possible further use of the framework, the Digital Green Certificate and personal data related to it at the Member States level must respect Art. 7 and Art. 8 of the EU Charter of Fundamental Rights and must comply with the GDPR, including Art. 6(4) GDPR. This implies the need for a proper legal basis in Member State law, complying with the principles of effectiveness, necessity, proportionality and including strong and specific safeguards.

Adopted: 31 March 2021

### **5.5.9. EDPB-EDPS Joint Opinion 05/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)**

*See Section 3.4 for a full summary.*

The European Commission presented its Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) on 21 April 2021. In their joint opinion, the EDPB and the EDPS welcome the concern of the legislator in addressing the use of artificial intelligence (AI) within the EU and stress the important data protection implications of the future regulation. Relevant issues include the following: the Proposal's scope, a risk-based approach, prohibited uses of AI, high-risk AI systems, governance and the European AI Board, and its interaction with the data protection framework.

Adopted: 18 June 2021

### **5.5.10. Statement 02/2021 on new draft provisions of the Second Additional Protocol to the Council of Europe Convention on Cybercrime (Budapest Convention)**

Following the previous EDPB contribution to the draft Second Additional Protocol to the Council of Europe Convention on Cybercrime (Budapest Convention), the EDPB adopted a statement on the new draft provisions to provide its expertise with a view to ensuring that data protection matters are duly considered in the overall drafting process of the Additional Protocol.

The statement focuses on assessing draft provisions that have not been subject to previous stakeholder consultations, such as joint investigations and their respective teams, expedited disclosure of stored computer data in an emergency, and request for domain name registration information.

The EDPB notes that the new draft provisions are likely to affect the conditions for access to personal data in the EU for law enforcement purposes and, consequently, it calls on the relevant EU and national institutions to carefully scrutinise the ongoing negotiations. The goal of such action is to guarantee full consistency of the proposed Second Additional Protocol with the EU acquis in the field of personal data protection.

Adopted: 2 February 2021

### **5.5.11. Statement 03/2021 on ePrivacy Regulation**

The EDPB adopted a statement on the draft ePrivacy Regulation where it welcomes the agreement on the negotiation mandate by the Council of the EU as a positive step in the finalisation of the ePrivacy Regulation. The statement expresses concerns about proposed rules on the retention of electronic communication data for the purposes of law enforcement and safeguarding national security. It further recalls the necessity of a specific EU regulation protecting the confidentiality of electronic communications. The upcoming Regulation must enforce the consent requirement for cookies and similar technologies, and enable technical tools allowing consent to be easily obtained.

The EDPB reiterates that competent national SAs responsible for enforcing the GDPR should be entrusted with the oversight of the privacy provisions of the future ePrivacy Regulation in order to ensure harmonised interpretation and enforcement of the ePrivacy Regulation across the EU and to guarantee a level playing field in the Digital Single Market. The EDPB also underlines the practical difficulties that will be faced in case

national competent authorities who are not members of the EDPB would have to interact with the EDPB.

Adopted: 9 March 2021

### **5.5.12. Statement 04/2021 on international agreements including transfers**

The EDPB calls upon the EU Member States to assess and, where necessary, review their international agreements that involve international transfers of personal data and were concluded before 24 May 2016 (for those relevant to the GDPR) and 6 May 2016 (for those relevant to the Law Enforcement Directive (LED)). These actions should be performed to ensure alignment, where needed, with EU law, in particular the GDPR and the LED, CJEU case law on data protection, and relevant EDPB guidance.

Adopted: 13 April 2021

### **5.5.13. EDPB contribution to the 6th round of consultations on the draft Second Additional Protocol to the Council of Europe Budapest Convention on Cybercrime**

The EDPB submitted comments on the draft Second Additional Protocol to the Council of Europe Cybercrime Convention Committee (T-CY) during its sixth consultation round.

From an EU data protection law point of view, the draft Protocol, as per its level of norm, provisions and legal effect, would be applicable to the disclosure and transfer of personal data from the EU to third countries. In relation to the draft Art. 13 of the Protocol ("Condition and safeguards"), the EDPB recommends that the application and implementation of the principle of proportionality be included in the text. The EDPB could not provide a full assessment on the draft text of Art. 14 ("protection of personal data") due to the non-publication of the explanatory report for this provision.

The EDPB recommends clarifying the application of some of the principles and procedures that Art. 14 contains, such as its scope, purpose and use of personal data received by the requesting party, the processing of sensitive data, retention periods, automated decisions, maintaining of records, onward sharing, onward transfer, transparency and notice, rights of data subjects, oversight and suspension.

The EDPB calls on the T-CY members and protocol drafters to amend the draft provisions presented for consultation to ensure the finalised protocol is fully compatible with EU primary and secondary law, guaranteeing that the level of protection of personal data as per EU law is not undermined.

Adopted: 4 May 2021

## 5.5.14. Statement 05/2021 on the Data Governance Act in light of the legislative developments

In pursuit of reinforcing its main remarks from the EDPB-EDPS Joint Opinion on the Data Governance Act (DGA) ([see Section 5.5.7 for a full summary](#)), the EDPB adopted this statement on the DGA concerning the developments in the legislative process.

The EDPB states that it is important to have robust data protection safeguards, as a lack of safeguards creates a risk that the trust in the digital economy would not be sustainable. There is a need to ensure consistency between the DGA and the EU data protection acquis. Certain aspects are particularly important, such as the provision in the DGA of a clear interplay between the DGA and the GDPR, the alignment of the definitions and terminology of the DGA with the ones of the GDPR, and the clarification of the appropriate legal basis regarding the processing of personal data.

Adopted: 19 May 2021

## 5.5.15. EDPB contribution to the 6th round of consultations on the draft Second Additional Protocol to the Council of Europe Budapest Convention on Cybercrime

On 8 July 2020, the European Commission submitted to the EDPB a request focusing on health research and provided a list of concrete questions related to data protection for health related research.

In its replies, the EDPB states that ethics standards cannot be interpreted in such a way that only explicit consent of data subjects can be used to legitimise the processing of health data for scientific research purposes. Art. 6 and Art. 9 GDPR contain other options for a legal basis and an exemption, which can be relied on for processing of health data for scientific research purposes. In its replies the EDPB provides clarifications on data protection related concepts, such as the processing of previously collected health data, the notion of broad consent, transparency, data safeguards, large scale processing and international cooperation.

The EDPB response constitutes only a preliminary position on the topic. In its forthcoming guidelines on processing personal data for scientific research purposes, the EDPB will elaborate further on these issues while aiming at providing a more comprehensive interpretation of the various provisions in the GDPR that are relevant for the processing of personal data for scientific research purposes.

Adopted: 2 February 2021

## 5.6. OTHER GUIDANCE AND INFORMATION NOTES

### 5.6.1. Pre-GDPR BCRs overview list

The EDPB published an [updated list of pre-GDPR BCRs](#) on its website. This list provides information on BCRs that were

submitted to SAs in accordance with the rules applicable under Directive 95/46 and for which the procedure for approval ended prior to 25 May 2018, when the GDPR started applying. The list notes 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.

Adopted: 26 January 2021

### **5.6.2. Statement on the withdrawal of the United Kingdom from the European Union - update 13/01/2021**

The second version of the Statement, adopted on 13 January 2021 (the first having been adopted on 15 December 2020), was updated taking into consideration that on 15 December 2020, an agreement on future relations was reached between the EU and the UK. The EDPB reminds all stakeholders that the 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 the GDPR and UK entities will not be considered as transfers to a third country subject to the provisions of Chapter V GDPR. This interim provision could be applied for a maximum period of six months (i.e. until 30 June 2021 at the latest). The EDPB specifies that, as of 1 January 2021, the One-Stop-Shop (OSS) mechanism is no longer applicable to the UK, so the UK Information Commissioner's Office is no longer part of it.

The EDPB emphasises that the decision to benefit from the unified dialogue enabled by the OSS mechanism in cross-border processing cases is up to the individual controllers and processors, who to that end could decide whether to set up a new main establishment in the EEA under the terms of Art. 4(16) GDPR. The EDPB recalls that controllers and processors not established in the EEA, but whose processing activities are subject to the application of the GDPR under Art. 3(2)

GDPR, are required to designate a representative in the EU in accordance with Art. 27 GDPR.

Adopted: 13 January 2021

### **5.6.3. Information note on data transfers under the GDPR to the United Kingdom after the transition period - update 13/01/2021**

By the time of the second version of the note, adopted on 13 January 2021, an agreement had been reached between the EU and the UK on 24 December 2020. The agreement provided that for a maximum period of six months from its entry into force – i.e. until 30 June 2021 at the latest – and upon the condition that the UK's current data protection regime stays in place, all flows of personal data between stakeholders subject to the GDPR and UK organisations would not be considered as international transfers.

Until 30 June 2021, at the latest, organisations subject to the GDPR would be able to carry on transferring personal data to UK organisations without the need to either put in place a transfer tool under Art. 46 GDPR or rely on an Art. 49 GDPR derogation. If no adequacy decision applicable to the UK as per Art. 45 GDPR would be adopted by 30 June 2021 at the latest, all transfers of personal data between stakeholders subject to the GDPR and UK entities would then constitute a transfer of personal data to a third country.

Adopted: 13 January 2021

## **5.7. PLENARY MEETINGS AND SUBGROUPS**

In the period between 1 January and 31 December 2021, the EDPB held 15 plenary meetings. The [agendas](#) and [minutes](#) of these meetings are published on the EDPB website. The outcome of the plenary meetings consists of adopted guidelines, opinions and other documents such as statements

or information notes to advise the European Commission, national SAs and other stakeholders on data protection matters, with a primary focus on the GDPR. Additionally, there were 200 expert subgroup meetings. In total, 389 meetings were held, including plenary meetings, expert subgroup meetings and drafting team meetings.

The different expert subgroups focus on specific areas of data protection and assist the EDPB in performing its tasks. Chapter 8 outlines the list of the expert subgroups and their respective mandates.

## 5.8. STAKEHOLDER CONSULTATION

### 5.8.1. Stakeholder events

The EDPB organises stakeholder events to gather input and views on specific issues in the interest of developing future guidance. In 2021, the EDPB organised such an event on processing personal data for scientific research purposes on 30 April. The event took place online and secured approximately 60 participants that represented a combination of academia, NGOs, commercial organisations and SAs. They shared their experience concerning the use of personal data for scientific research purposes and emphasised areas that needed further clarifying or explaining. Alongside this provided input, the EDPB gathered further valuable insights on the topic from a questionnaire sent to both parties who attended and could not attend prior to the event. The EDPB will use all the provided stakeholder input in the context of drafting future guidance on data processing for scientific research purposes.

### 5.8.2. Public consultation on draft guidance

Following the preliminary adoption of guidelines, the EDPB organises public consultations to give stakeholders and citizens the opportunity to provide additional input. The EDPB Members and the EDPB Secretariat in charge of drafting the guidelines consider this input in the subsequent drafting process. The guidelines are then adopted in their final version.

To further enhance transparency, the EDPB publishes on its website stakeholders' contributions to public consultations. In 2021, the EDPB launched several such consultations:

- In January, the EDPB opened public consultations on [Guidelines 01/2021 on Examples regarding Data Breach Notification](#). There were 32 contributions made to the guidelines, mostly submitted by business organisations and associations or DPO entities.
- In March, [Guidelines 02/2021 on Virtual Voice Assistants](#) were open for public consultations. They attained eighteen contributions from a mix of different entities, such as academic and research institutions and business associations.
- Later in April, the EDPB opened public consultations on both [Guidance on certification criteria assessment \(Addendum to Guidelines 1/2018 on certification and identifying certification criteria in accordance with Arts. 42 and 43 of the Regulation\)](#) and [Guidelines 03/2021 on the application of Art. 65\(1\)\(a\) GDPR](#). The Guidance on certification criteria assessment received contributions from six entities, mainly comprising individuals, academia and public authorities. The Guidelines 03/2021 on the application of Art. 65(1)(a) GDPR received three contributions from a variety of entities.
- The EDPB published [Guidelines 04/2021 on codes of conduct as tools for transfers](#) for consultation in July. There were ten contributions to these guidelines.



- In November, the EDPB launched public consultations on Guidelines 05/2021 on the Interplay between the application of Art. 3 and the provisions on international transfers as per Chapter V of the GDPR, which were accepting contributions until 31 January 2022.

### 5.8.3. Survey on practical application of adopted guidance

For the fourth year in a row, the EDPB conducted a survey as part of the annual review of the EDPB's activities under Art. 71(2) GDPR. Questions centred on the EDPB's work and output in 2021, with a focus on its guidelines and recommendations, all with a view to understanding the extent to which stakeholders find the EDPB's guidance helpful in interpreting the GDPR's provisions, and in order to identify future paths to better support organisations as they interact with the EU data protection framework.

#### 5.8.3.1. Participants and methodology

The survey compiles the views of various entities with different interests and concerns related to EU data protection law. Stakeholders consulted included representatives from an EU DPO organisation, representing a network of national associations of data protection and privacy officers. Accordingly, a representative and comprehensive view of the sector was obtained. Stakeholders also included academia and NGOs in the field of data protection and privacy rights. This allowed for a broad representation of actors from different sectors. The EDPB used semi-structured, one-on-one virtual interviews to consult participants. The questions were based on a standardised questionnaire. From this, data was synthesised and commonalities identified.

#### 5.8.3.2. Findings

The surveyed stakeholders indicated that the EDPB guidelines and recommendations are generally coherent and helpful in interpreting ambiguous data protection rules and better understanding data protection rights and duties. The structure of the documents also provides for easy navigation through the content, with Guidelines 01/2021 on data breach notifications receiving praise in this respect.

Most stakeholders consulted the guidelines and recommendations on a near daily basis for work purposes.

Stakeholders indicated the need for quicker adoption of new guidelines and recommendations. In addition, they suggested that shorter documents with comprehensive executive summaries would be useful. When certain guidance documents become very long, a suggestion was made for the EDPB to consider issuing a complementary, shorter version of the final document. With respect to content, stakeholders saw high practical value in the examples outlined in the EDPB guidelines and hoped to see this practice continue.

The surveyed stakeholders actively participated in the consultative processes of the EDPB throughout 2021. Some participants suggested they would appreciate a clearer outline of how their proposed input was incorporated into guidelines adopted after consultation.

Overall, due to the improved website and consultation processes, the participants found significant improvement in the communication and transparency of the EDPB. Stakeholders stated that in light of consistency and compliance, they followed and acted in accordance with the EDPB's guidance.

The EDPB highly appreciates the stakeholders' participation and useful contribution to its work. Feedback on the guidance's operational value and alignment with other EU laws was equally appreciated as it gave actionable insights into stakeholder needs. The provided feedback on communication and transparency is also beneficial for future stakeholder engagement and initiating plans of action. Overall, the EDPB plans to continue upholding and building upon the consistency of its work in the future.

### 5.9. EXTERNAL REPRESENTATION OF THE BOARD

Public awareness and cooperation are vital to upholding data protection rights in the EEA and beyond, which is why the EDPB values stakeholder and citizen engagement. The EDPB Secretariat supports the Chair and Deputy Chairs in engagements with other EU institutions or bodies, and when they represent the EDPB at conferences and multi-stakeholder platforms. Staff members from the EDPB Secretariat also take part in several events to present the activities of the EDPB.

#### 5.9.1. Participation of Chair and Deputy Chairs in conferences and speaking engagements

In 2021, the Chair of the EDPB, Andrea Jelinek, had over nineteen speaking engagements, which for the most part were remote. The speaking engagements included press briefings, presentations and panel discussions for a range of institutes, academic forums and policy agencies. The Chair also met with European Commissioners and representatives from, among others, UNESCO and the Council of the EU Working Party on Information Exchange and Data Protection. In addition, she participated in several conferences and summits on data protection and privacy matters.

The EDPB Deputy Chair Ventsislav Karadjov took part in nine speaking engagements, most of which were remote. They consisted of speeches, presentations and panel discussions at

several conferences and forums. The EDPB Deputy Chair Aleid Wolfsen participated in three remote speaking engagements. His engagement comprised speeches, presentations and panel discussions at different events.

#### 5.9.2. Participation of EDPB Staff in conferences and speaking engagements

EDPB staff represented the EDPB at 33 events, both in-person and remotely. The events were hosted by, amongst others, universities, trade associations and EU institutions. Their engagement at these events consisted of discussing achievements, challenges and potential solutions to current data protection issues, but also disseminating educational knowledge of data protection and privacy for tailored made courses at different universities.



# 6



## SUPERVISORY AUTHORITY - ACTIVITIES IN 2021

Under the GDPR, national Supervisory Authorities (SAs) have a duty to cooperate to ensure the consistent application of data protection law. In cases that have a cross-border component, the SAs of the European Economic Area (EEA), i.e. the 27 EU Member States plus Iceland, Norway and Liechtenstein, have a range of tools at their disposal to facilitate harmonisation.

These tools are:

- Mutual assistance;
- Joint operations;
- The One-Stop-Shop cooperation mechanism.

### 6.1. CROSS-BORDER COOPERATION

The GDPR requires the EEA SAs to cooperate closely to ensure the consistent application of the GDPR and protection of individuals' data protection rights across the EEA.

One of their tasks is to coordinate decision-making in cross-border data processing cases.

#### 6.1.1. Preliminary procedure to identify the Lead and Concerned Supervisory Authorities

Before starting a One-Stop-Shop (OSS) procedure for a cross-border case, it is necessary to identify the Lead Supervisory Authority (LSA) and the other Concerned Supervisory Authorities (CSAs). The LSA leads the investigation and drafts

the decision, while the CSAs have the opportunity to raise objections.

The LSA is identified as the SA of the EEA country where the data controller or processor under investigation has its main establishment. To identify a controller's or processor's main establishment, one key criterion is the place of central administration. Further information on this subject is available in the [Article 29 Working Party Guidelines for identifying a controller's or processor's LSA](#), endorsed by the EDPB at its first plenary meeting on 25 May 2018.

The EDPB created workflows in the Internal Market Information System (IMI) to enable SAs to identify their respective roles. This IT platform is used to support cooperation and consistency procedures under the GDPR. The main purpose of this procedure is to define roles at an early stage.

In case of conflicting views regarding which SA should act as LSA, the EDPB acts as a dispute resolution body and issues a binding decision. From 1 January 2021 to 31 December 2021, there were 553 instances in which LSAs and CSAs were identified.

### 6.1.2. Database regarding cases with a cross-border component

A case with a cross-border component is registered in a central database via the IMI and may occur in several situations:

- When the data controller or processor has an establishment in more than one Member State;
- When the data processing activity substantially affects individuals in more than one Member State; and/or
- When SAs are simply exchanging information, i.e. providing each other with mutual assistance.

Between 1 January and 31 December 2021, there were 506 entries in the database out of which 375 originated from a complaint, while 131 had other origins, such as investigations, legal obligations and/or media reports.

Please note that:

- References to case register entries in these statistics do not have a 1-to-1 correlation to the number of cross-border complaints handled per country as multiple complaints may be bundled in one case register entry which therefore can relate to multiple cross-border cases;
- Depending on the Member State legislation, supervisory authorities may have handled complaints outside of the Art 60 procedure in accordance with their national law.

### 6.1.3. One-Stop-Shop mechanism and decisions

The OSS mechanism demands cooperation between the LSA and the CSAs. The LSA leads the investigation and plays a key role in the process of reaching consensus between the CSAs, in addition to working towards reaching a coordinated decision about the data controller or processor.

The LSA must first investigate the case while taking into account national procedural rules, ensuring that the affected individuals can exercise their rights. The LSA can gather information from another CSA via mutual assistance or by conducting a joint investigation. The IMI system also gives the LSA and other CSAs at any point the opportunity to informally communicate with each other to collect and exchange relevant information.

Once the LSA has completed its investigation, it prepares a draft decision, which it then communicates to the CSAs. They have the right to object. An objection either leads to a revised draft decision or, if no route to consensus can be found, the EDPB acts as a dispute resolution body and issues a binding

decision. The LSA must adopt its final decision on the basis of the EDPB's decision. If the CSAs do not object to either the initial draft or the revised decision, they are deemed to agree with the draft decision.

Between 1 January 2021 and 31 December 2021, there were 209 draft decisions, which resulted in 141 [final decisions](#).

The IMI offers different procedures that can be followed when handling OSS cases:

- Informal consultation procedures;
- Draft decisions or revised decisions submitted by the LSA to the CSAs; and/or
- Final OSS decisions submitted to the CSAs and the EDPB.

The EDPB maintains a public [register](#) of the final decisions taken by LSAs and complaint receiving SAs pursuant to the OSS as a valuable resource to showcase how SAs work together to practically enforce the GDPR. The register offers an exceptional opportunity to read final decisions taken by, and involving, different SAs in a cross-border context. These decisions often contain important guidance on how to comply with the GDPR in practice. The register contains both final decisions and summaries prepared by the EDPB Secretariat and duly approved by SAs. The relevant SAs have validated the information in the register in accordance with the conditions provided by their national legislation.

This section contains a selection of examples of Art. 60 GDPR final decisions taken from the EDPB's public register. The first section contains some cases where SAs handed out administrative fines in accordance with Art. 83 GDPR when data controllers did not comply with the GDPR. The second section provides summaries of some other final decisions in cases where SAs did not issue administrative fines, but provided guidance on the interpretation of specific provisions of the GDPR.

The Annual Report references certain final decisions from 2021, but also includes one from late 2020.

### 6.1.3.1. Selection of cases involving administrative fines

Consistent enforcement of data protection rules is central to a harmonised data protection regime. Once an infringement of the GDPR has been established based on the assessment of the facts of the case, the competent SA must identify the most appropriate corrective measure to address the infringement. Administrative fines are one of the most powerful enforcement measures the SAs can adopt, together with the other measures in Art. 58 GDPR.

#### LSA: Dutch SA

##### **Personal data breach / Notification of a personal data breach to the supervisory authority / Administrative fines**

Year of decision: 2020<sup>3</sup>

OSS register number: EDPBI:NL:OSS:D:2020:173

On 7 February 2019, the service provider of an online platform notified the LSA of a personal data breach that it had discovered on 10 January 2019. The controller indicated in its notification that an unknown third party had gained access to personal data in the controller's reservation system which are used by the platform's partners to manage the reservations. As a result, the personal data of various data subjects who had made reservations via the controller's platform were compromised. The LSA then commenced an investigation on the controller's compliance with Art. 33(1) GDPR.

During its investigations, the LSA found that the controller had been informed on 8 January 2019 by one of its partners that, following a possible personal data breach in the reservation system, an unknown third party had contacted customers and pretended to be affiliated with the controller, once as an

employee of the controller and other times as an employee of one of the partner organisations on the platform. The LSA noted that the controller received two similar complaints from the same provider on 13 January 2019 and 20 January 2019; and that on 20 January 2019, a second partner reported the same type of incident. The LSA noted that, despite the reports about these several incidents, the controller's entity in charge of the receipt of these incidents did not notify the controller's security team until 31 January 2019. After having conducted investigations, the controller's security team informed the controller's privacy team on 4 February 2019.

In view of the circumstances in which the incidents were reported to the controller by the partners, the LSA found that the controller was deemed to have knowledge of the personal data breach at least on 13 January 2019, as the information given by the partner indicated with a reasonable degree of certainty that personal data had been compromised. As a result, the LSA pointed out that the controller should have notified the LSA of the personal data breach by 16 January 2019 at the latest. It is an established fact that the controller only made this notification on 7 February 2019, i.e. 22 days too late. The same applies if 20 January 2019 should be adopted as the starting date, then the notification was done 15 days too late compared to the deadline of 72-hour set out by Art. 33(1) GDPR.

The LSA stressed that the controller's argument that the delay in notifying the data breach was due to a failure by a single part of the controller's organisation to report the incident to the security team, as per the controller's internal procedure, is without effect. The LSA also stressed that, by choosing to carry out an in-depth investigation instead of notification in phases, the controller did not comply with the rules laid down in Art. 33(3) GDPR.

The controller had informed and advised the data subjects about taking measures to reduce the potential damage. The controller had declared itself willing to compensate any damages (suffered or to be suffered) by the data subjects. The controller also immediately informed its affected partners and placed warnings on the website.

The LSA imposed an administrative fine of EUR 475,000 on the controller for the infringement of Art. 33(1) GDPR.

<sup>3</sup>. Decision adopted in late 2020, so included in 2021 Annual Report.

### **LSA: Dutch SA**

#### **Personal data breach / Data security / Administrative fines**

Year of decision: 2021

OSS register number: not available yet

On 24 October 2019, the LSA received a notification from a controller regarding a personal data breach indicating that a malicious third party had gained unauthorised access to the controller's systems. The LSA also received three follow-up notifications. The LSA was informed that the controller had discovered the breach on 21 October 2019 and had immediately engaged an external service provider to block the attacker and to prepare a forensic report analysing the affected systems and the personal data involved. According to the forensic analysis, the attacker had focussed on exploratory activities but had also copied network documentation, business and other documents, as well as six mailboxes to a remote location. The mailboxes had been found to contain files with personal data. On 25 February 2020, 81,000 data subjects (employees and customers of the controller) were notified of the breach. The personal data affected included first name, last name, date of birth, flight information, booking number, luggage information, as well as wheelchair requirements. For

(potential) employees, more data were affected, including, resumes and business contact information.

The LSA concluded that, at the time of the breach, the controller was processing personal data of over 25 million individuals. Of these, personal data of up to 83,000 individuals and health data of 367 individuals were leaked. According to the controller, 90% of the affected data subjects are Dutch, based on the point of sale. The controller could not provide a breakdown of other countries of origin but considering the amount of information, the LSA decided that 10% still amounts to data subjects from other EU countries being substantially affected.

The LSA investigated whether the technical measures taken by the controller with regard to access to personal data were appropriate as required by Art. 5(1)(f) GDPR in conjunction with Art. 32 GDPR. It was determined that the attacker had used a “password spray” or “credential stuffing” attack, i.e. applied, frequently used or previously leaked passwords. The cause of the breach was a simple and frequently used password that was easy to guess by automated means. The password strength and level were not in accordance with the authentication policy of the controller. Furthermore, the periodic security checks conducted by the controller had shown that the controller’s password policy had not been adhered to. In addition, the LSA considered that dividing the controller’s network into several segments could have prevented the attacker from gaining further access to the controller’s systems and that users’ privileges could have been better adjusted. Given the state of the art and the implementation costs, the LSA considered that the technical measures implemented at the time of the breach were not appropriate within the meaning of Art. 32 GDPR.

The LSA imposed on the controller an administrative fine of EUR 400,000 for the infringement of Art. 32(1) and (2) GDPR.

### LSA: Spanish SA

#### **Personal data breach / Hacker-attack / Data security / Administrative fines**

Year of decision: 2021

OSS register number: EDPBI:ES:OSS:D:2021:239

The controller, a company owning a web platform, was hit by several cyber-attacks from an unidentified third party who accessed its database hosted on the platform of a cloud service provider. On 29 June 2018, the controller notified the LSA of a first cyber-attack, which occurred on 27 June 2018 and resulted in the unauthorised access to the personal data of 232,766 customers residing in more than 170 countries (comprising almost all EU member states). On 27 July 2018, the controller notified the LSA of a second data breach, which occurred on 25 July 2018, and resulted in the unauthorised access of the usernames and email addresses of 2,892,786 account holders. In response to these data breaches, the controller implemented several technical and organisational corrective measures.

Following the notification of the two data breaches, the LSA initiated investigations into a possible breach of Arts. 32, 33 and 34 GDPR. As a result of these investigations, the LSA found that the controller failed to implement up-to-date technical and organisational security measures, taking into account the degree of risk of the processing activities carried out. Considering that these security deficiencies were to a large extent responsible for the occurrence of the above-mentioned incidents, the LSA ruled that the company infringed Art. 32(1) GDPR. Nonetheless, the LSA pointed out that the company notified the breaches in accordance with its obligation under Art. 33 GDPR. Finally, in light of the evidence at hand, the LSA concluded that there was no high risk to the

rights and freedoms of natural persons that would require informing data subjects in accordance with Art. 34 GDPR.

The LSA imposed an administrative fine of EUR 100,000 on the controller for the infringement of Art. 32(1) GDPR.

### **LSA: French SA**

#### **Personal data breach / Data security / Passwords / Data subject rights / Administrative fines**

Year of decision: 2021

OSS register number: EDPBI:FR:OSS:D:2021:181

Following the notification of a personal data breach on the controller's website affecting 210,692 European nationals, the LSA conducted both on-site and online audits of the controller to verify its compliance with the GDPR. Thereafter, the LSA also carried out a second on-site control in the context of the LSA's investigations regarding five complaints received from customers and prospects concerning the commercial prospecting by the controller they have been subject to, as well as the exercise of their rights.

The LSA found that the controller did not facilitate the exercise of data subject rights, as the email address provided to them for this purpose was defective. In addition, the LSA pointed out the complexity of the right of access procedure implemented by the controller for prospects receiving postal solicitations. Therefore, the LSA considered that the controller failed to comply with its obligations under Art. 12(2) GDPR.

Following its investigations regarding the data breach notification, the LSA found that the controller had failed to ensure the security of the personal data it processed. Firstly, the LSA found that the controller did not ensure the effectiveness of the technical and organisational measures implemented by its processor. In this regard, the LSA

concluded that the controller should have been more vigilant in complying with security standards considering that it had already been sanctioned by the LSA for security issues involving the same processor. Finally, the LSA considered that the controller's requirements regarding the robustness of passwords, when it comes to their length and complexity, were insufficient to ensure the security of the personal data processed and to prevent third parties from accessing the personal data. The LSA recommended that a password have at least 12 characters - containing at least one capital letter, a lower-case letter, a digit and a special character - or at least eight characters - containing three of these four characters - if it is accompanied by an additional measure, such as the timing of access to the account after several failures, setting up a mechanism to guard against automated and intensive attempts and/or blocking the account after several unsuccessful authentication attempts. The LSA imposed an administrative fine of EUR 250,000 on the controller. In addition, the LSA imposed a compliance order on the controller to remedy its breaches of Art. 12 and Art. 32 GDPR with a penalty payment of EUR 500 per delayed day, starting from the end of a period of three months following the notification of the decision.

### **LSA: French SA**

#### **Transparency / Right to erasure / Data security / Passwords / Administrative fines**

Year of decision: 2021

OSS register number: EDPBI:FR:OSS:D:2021:279

The LSA carried out a volition audit at the premises of a controller in order to verify its compliance with the GDPR. The audit focused on the processing of personal data relating to the company's current and prospective customers. More specifically, the LSA investigated the information provided to

data subjects, compliance concerning data subjects' rights and data retention periods. In order to complete these investigations, the LSA also carried out an online audit relating to all processing accessible from the controller's website, with a particular focus on, among other issues, the methods used for informing data subjects.

In the course of its investigation, the LSA noted that the active database of the controller contained personal data of 16.653 persons who had not placed an order in more than 5 years and 130,000 persons who have not signed into their customer account in more than 5 years. In this regard, the LSA ruled that, although the controller implemented a retention period policy, personal data were kept for much longer periods than those specified in this policy on the day of the audit and did not appear to be appropriate for the purposes for which the data were processed (Art. 5(1)(e) GDPR). Furthermore, following its on-site and online audits, the LSA found that certain mandatory information provided for by Art. 13 GDPR was missing, namely the contact details of the DPO, the data retention periods, the legal basis of the processing and information on certain data protection rights. Nonetheless, the LSA noted that the company had complied with all the points raised regarding the information of data subjects by the end of the investigation.

As to the controller's obligation to comply with requests to delete personal data (Art. 17 GDPR), the LSA found that when an individual requested the deletion of its account, the company simply deactivated the account in question. In this regard, the LSA stressed that the email address used for marketing purposes should have been deleted in the event of withdrawal of consent insofar as its retention is not legitimate on any other basis. The company took measures in the course of the procedure, but did not fully achieve compliance, so the LSA issued an injunction against the company.

Finally, the LSA found that the format of passwords when both creating an account on the controller's website and accessing the customer databases were insufficiently robust to ensure data security within the meaning of Art. 32 GDPR. The LSA found further infringements of the same provision due to the obsolete nature of the hash function used for the storage of passwords of employees using the controller's website and the use of the same account by several employees when accessing a copy of the controller's production database.

The LSA imposed an administrative fine of EUR 300,000 to the controller for breaching Art. 5(1)(e), Art. 13, Art. 17 and Art. 32 GDPR. In addition, the LSA imposed a compliance order on the controller to remedy its breach of Art. 5(1)(e) GDPR with a penalty payment of EUR 500 per delayed day, starting from the end of a period of three months following notification of the decision.

### **LSA: Lithuanian SA**

#### **Personal data breach / Data security / Publicly available data / Administrative fines**

Year of decision: 2021

OSS register number: not available yet

The LSA started inspections on its own initiative upon receiving information that personal data of 111,052 customers of the controller (among which 433 residing in other EU countries), including personal identification numbers, had been made publicly available. The LSA subsequently received a data breach notification and additional information from the controller.

The case was opened on the basis of a motion for imposition of an administrative fine sent by the LSA to the controller on 25 May 2021. The motion established that the personal data made public had been received from the backup copy of a

database stored in the controller's online storage without protection. The unprotected database had been created on 27 February 2018, meaning that the breach had existed from this date until 16 February 2021 when the controller suspended external access to the database, hence the applicability of the GDPR to the case. The controller provided clarifications with regard to the motion, alleging procedural irregularities, including the unreasonable extension of the investigation, the improper definition of the GDPR applicability to the case and factual errors, all of which the LSA considered and responded to in its final decision.

Analysis of the data stored in the database showed that personal data (names, driving licences, payment cards) had been stored in open text without encryption, and the passwords in the database encrypted with SHA-1 had been weak and unsafe. The controller had failed to purchase additional log record services for the database making it difficult to determine when and how many times customer data had been misappropriated. Considering this, the LSA found that the controller had performed post-breach security analysis (audits of firewalls, access rights, testing systems etc.) and had complied with Art. 33(3) GDPR. However, the LSA established that by failing to ensure proper access control and restrictions, by enabling third parties to access the file containing personal data without authorisation, by failing to ensure confidentiality of data stored in such file, by failing to record and store log records of access to and actions with the file, the controller had failed to comply with the requirements of Art. 32(1)(a) and (b) GDPR.

In addition, by failing to ensure proper management and control of the security of personal data, to appoint a competent person responsible for security and risk management, to segregate the duties and limits of responsibilities in the area of IT creation and maintenance from those in the area of cyber security, and to ensure recording, monitoring and assessment of access to and actions with the file, the controller had

violated the requirements of Art. 24(1) and Art. 32(1)(d) GDPR. As a result, the breach had created a risk to the rights and freedoms of natural persons, such as possible identity fraud, unlawful tracking, social engineering and others.

In light of the above, the LSA imposed on the controller an administrative fine of EUR 110,000 for breach of Art. 32(1)(a), (b) and (d) GDPR.

### 6.1.3.2. Selection of other cases on the interpretation of GDPR provisions

#### LSA: Latvian SA

##### Special categories of data / Biometrics / Fingerprints / Lawfulness of processing

Year of decision: 2021

OSS register number: not available yet

The LSA received information that a sports club is processing data subjects' (clients) fingerprints for customer identification in order to permit clients to enter the premises of the sports club. After investigating the circumstances of the incident, the LSA established that the controller used a biometric access control system in order to provide access control of clients to the sports club's premises. The LSA established that biometric data uniquely identifying natural persons were processed without a GDPR compliant legal basis and in disregard of the GDPR in regard to the principles of processing personal data. From 2016 until 2021, the controller processed biometric data of approximately 3,000 data subjects in order to ensure access control to the premises.

The LSA imposed an administrative fine of EUR 5,836 on the controller. The LSA also ordered the controller to delete the biometric data of clients (both existing and former), including a digital fingerprint point card created from a fingerprint

and to comply with the requirements of the GDPR. When imposing a fine, the LSA took into account the nature of the incident, the duration, the importance and purpose of the processing, the number of persons concerned, the conduct of the controller with a view to mitigating the damage suffered by the data subjects (the controller, following the LSA's request, ceased the processing of personal data), as well as the fact that the controller ensured cooperation with the LSA during the investigation.

#### **LSA: Cypriot SA**

#### **Special categories of data / Health data / Employment / Lawfulness of processing / Consent / Data minimisation**

Year of decision: 2021

OSS register number: EDPBI:CY:OSS:D:2021:175

The LSA investigated a complaint against the controller whose main activity is the provision of recruitment and placement services for cruise ships. Prior to starting work on a ship, the controller requests from employees to sign a general authorisation for the release of medical records in order to have access over them and be able to assist the employees with medical care, to arrange any associated travel and to handle any medical claim, in the event of a medical incident taking place on-board.

The LSA found that the authorisation appears to be based on the consent of the employee. However, the LSA considered that the condition of freely given consent was not fulfilled in the present case, as employees of the controller who are requested to sign the privacy notice in advance upon commencement of employment, had no real choice. Consequently, consent is not considered to be freely given when the employee is unable to refuse or withdraw his or her consent without detriment. The LSA recalled that in line with Art. 7(3) GDPR, the data subject shall have the right to

withdraw their consent at any time and the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. The LSA also considered that in the employment sector, in general, consent should not be used as the lawful basis for the processing due to the imbalance of the relationship between employer and employee. The LSA further stated that in line with the principle of data minimisation the controller should collect and generally process only data that are absolutely necessary to be able to assist the employees. The LSA was called upon to assess whether the controller could rely on another legal basis for the collection and general processing of employees' health-related data, other than consent. The LSA explained that the controller could possibly rely on Art. 9(2) GDPR, as it provides a list of possible exemptions to the ban on processing special categories of data, if certain additional conditions are fulfilled by the controller.

The LSA ordered the controller to cease the processing of health data of employees based on consent, to bring the processing into compliance with the provisions of the GDPR and in particular to take actions that consist of processing only the health-related data in the employment context which are necessary for the discharge of obligations laid down by law or by the collective agreements for the purposes of the recruitment, the performance of the contract of employment, health and safety at work, and the exercise and enjoyment of the rights and benefits of employees, as well as to inform the LSA on the actions taken to comply with its decision at the latest within one month from the date of the decision.



## LSA: Swedish SA

### Right to erasure / Legitimate interest / Payment data / Transparency and information

Year of decision: 2021

OSS register number: EDPBI:SE:OSS:D:2021:196

This case before the Swedish SA involved a complainant who previously had an account and a payment subscription to the controller's services. The complainant requested several times for his card details to be erased by the controller. According to the controller, it only processes unique identifiers for the payment cards or "instruments" (unique payment instrument identifiers) used by a customer when registering for free trial periods. The legal basis for the processing is legitimate interest. The controller considered that the continued processing of the data is not subject to the right to erasure because the controller has a strong, legitimate interest in continuing the processing that outweighs the rights and freedoms of the complainant, as the processing is necessary for the controller in counteracting fraud.

The LSA recalled that for processing to be based on Art. 6(1)(f) GDPR, all three conditions provided therein must be fulfilled. Firstly, the controller or third party has a legitimate interest (legitimate interest), secondly, the processing is necessary for purposes of legitimate interest (necessary) and third the interests or fundamental rights and freedoms of the data subject do not weigh heavier and require the protection of personal data (balance of interest). The LSA analysed the three conditions and in light of the reasons the controller had presented, the LSA found that the controller demonstrated compelling legitimate grounds that outweigh the complainant's interests, freedoms and rights. The controller thus had the right to continue processing the data after the complaint objected to the processing and the

complainant was therefore not entitled to erasure under Art. 17(1)(c) GDPR.

Nevertheless, the LSA concluded that the controller's response to the complainant had not been sufficiently justified pursuant to Art. 12(4) GDPR because the controller had not clearly stated what personal data is being processed, that the data is processed on the basis of a legitimate interest and what the legitimate interest is and that the answer did not contain information about the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy. The controller had thus processed personal data in violation of Art. 12(4) GDPR.

The LSA issued a reprimand to the controller.

## LSA: French SA

### Data subject rights / Data retention / Data security / Data processing agreements / Record of processing activities

Year of decision: 2021

OSS register number: EDPBI:FR:OSS:D:2021:202

This case involved a controller who runs a platform for rental vehicles, which puts vehicle owners in contact with private individuals. One of the controller's customers complained that his driving license was accessible via any browser with no authentication required, by entering an URL that connected to a software tool of the controller's subcontractor. The complainant stated that he had made several requests for deletion of his driving license but to no avail.

Upon investigation, the LSA found that although the controller had defined a policy on data retention periods, in practice there had been no restriction on the retention of data relating to the creation of users' accounts. According to the LSA, this constituted a breach of the obligations of Art. 5(1)(e) GDPR.

Furthermore, the LSA found that customer records created by the controller were not anonymised and it was still technically possible to re-identify customers from their user numbers by, for example, cross-referencing them with other indirectly identifying personal data. Therefore, the general data erasure procedure implemented by the controller did not guarantee data subjects' right to erasure and the controller breached Art. 17 GDPR.

The controller had entrusted verification of the identities of its users' profiles to two service providers processing personal data on its behalf. However, the relevant service provision contracts did not satisfy the requirements of Art. 28(3) GDPR. In addition, according to the LSA, although the controller had fewer than 250 employees, it was carrying out a variety of personal data processing operations regarding prospects and customers on a regular basis and for purposes such as marketing, customer management and combating fraud. Despite that, the controller did not keep a record of processing activities and breached Art. 30 GDPR. Finally, the controller did not implement appropriate security measures to protect from potential unauthorised access to the supporting documents sent by users via email and retained the passwords to over 150,000 user accounts in a form that did not ensure their confidentiality. The LSA also found that the way of communicating data in response to access requests was exposing the data to a risk of compromise in the event of an attacker's intrusion into the data subject's inbox or interception of emails by an unauthorised third party.

The LSA ordered the controller to comply with the above-mentioned GDPR provisions and to adopt, within three months, the following measures: define and implement a policy on retention periods for its customers' and prospects' data, define and implement an effective procedure for the right to erasure, complete the contracts with the data processors by including the missing terms, keep a record of processing activities, take all necessary security measures, so

as to ensure the security of the data and prevent unauthorised third parties from accessing them.

### **LSA: Icelandic SA**

#### **Personal data breach / Data security / Education**

Year of decision: 2021

OSS register number: EDPBI:IS:OSS:D:2021:216

This case of the Icelandic SA involved a controller which is a company developing and operating an online information system intended for schools and other entities working with children, which allows for information exchanges between schools and parents. The case was opened after the controller informed the LSA via telephone of a data breach that had occurred in February 2019 due to a vulnerability within the online information system. The breach was made on purpose, by one of the students' parents, who wanted to expose faulty security within the system. The parent was able to access data from 423 students in 90 schools in Iceland while logged in, by using a script creating a random number in the visible web page address number found in the URL-bar (address-bar) of each student's personal page. Students' names and profile pictures and in some instances national identification numbers of students and/or their custodians were disclosed. The parent also contacted another person with access to the same system in Sweden who was able to access the national identification number and avatar of one child in Sweden.

The controller stated that, immediately after becoming aware of the breach, it had activated an action plan and had informed the principals of every elementary school in Iceland. The LSA carried out an investigation and found, on the basis of the information and data provided by the controller, that human error led to the data breach since a solution for the vulnerability, which had already been created, had not been fully implemented. Insufficient follow-up and

testing of security measures then led to this fact not being discovered until after the data breach had already occurred. The LSA concluded that the controller did not comply with the requirements of Art. 32(1)(b) and (d) GDPR, Art. 5(1)(f) GDPR and the relevant national law provisions.

Additionally, the controller did not ensure proper security of personal data of the data subjects affected by the data breach, because it had mistakenly sent national identification numbers to the wrong schools and data protection officers and therefore did not comply with Art. 5(1)(f) GDPR and relevant national law provisions.

The LSA imposed an administrative fine of ISK 3,500,000 (approximately EUR 238,475) on the controller.

### **LSA: Berlin SA**

#### **Right to erasure / Lawfulness of processing**

Year of decision: 2021

OSS register number: EDPBI:DEBE:OSS:D:2021:229

On 29 April 2018, a complainant requested the controller to erase his personal data and to close his customer account. The controller confirmed to the complainant the erasure by an email on 30 April 2018. In spite of this confirmation, the complainant submitted that a few months later he received an email from the controller informing him that the email address of his customer account had been changed. The complainant contacted the controller again, insisting that his customer account should have been erased. The account was finally erased on 26 March 2019.

In the course of its communication with the LSA, the controller explained its procedure applicable to requests for erasure and stated that the delay in the current case could have been due to obstacles, which were no longer possible

to assess. In addition, the controller claimed that the alleged violation should have been assessed in light of the national law applicable prior to the GDPR's entry into application.

The LSA first explained that although the failure to erase the complainant's personal data is a processing that started before the 25 May 2018, the GDPR applies because the complainant's request was not complied with until 26 March 2019. Therefore, the lawfulness of the processing of personal data has to be assessed in light of the GDPR.

The LSA found that the failure to erase the complainant's customer account constituted a violation of Art. 17(1)(a) and (b) GDPR, in conjunction with Art. 6(1) and Art. 5(1) GDPR. It recalled that if one of the grounds listed in Art. 17(1) GDPR applies, the controller has to erase the complainant's data immediately, i.e. without undue delay. The LSA also found that the controller could not successfully invoke any of the exceptions under Art. 17(3)(e) GDPR.

First, regarding the violation of Art. 17(1) GDPR, the LSA concluded that with the declaration of the request for erasure on 29 April 2018, the purpose of processing had ceased to exist and erasure was possible on the basis of Art. 17(1)(a) GDPR. By requesting the closure of his customer account, the complainant had initiated the end of the customer relationship, so continued storage of the data was no longer necessary within the meaning of Art. 6(1)(b) GDPR. In addition, according to the LSA, the data subject was entitled to request deletion of his personal data based on Art. 17(1)(b) GDPR too, since the request for erasure implicitly includes the withdrawal of consent within the meaning of Art. 7(3) GDPR. The retention of the personal data could not be based on Art. 6(1)(f) GDPR, as there was no overriding legitimate interest in not erasing the data and there were no actual indications for the existence of grounds for obstruction (e.g., outstanding invoices). Moreover, the controller could not successfully invoke any of the exceptions under Art. 17(3) GDPR.

Second, the LSA concluded that continued storage of the complainant's personal data also constituted a violation of Art. 6(1) GDPR because there was no legal basis for the continued storage of the data after the request for erasure. The controller bears the burden of proof for the existence of one of the conditions mentioned in Art. 6(1)(a) to (f) GDPR, which was not provided in the present case.

In light of the above, and since it could not be clearly established whether the e-mail address of the customer account had been changed before the request for erasure, the LSA issued a reprimand to the controller.

### **LSA: Spanish SA**

**E-commerce / Transparency / Lawfulness of processing / Data subject rights / Right to be informed / Right to object**

Year of decision: 2021

OSS register number: EDPB1:ES:OSS:D:2021:263

Following a data subject's complaint launched in Germany, the LSA found that the privacy policy of the controller's website was difficult to read due to a large number of grammatical and spelling errors, and that its structure was confusing. As a result, the LSA found that the privacy policy violated Art. 12(1) GDPR regarding the obligation to provide information to data subjects in a concise, transparent, intelligible and easily accessible form. Additionally, several shortcomings were identified by the LSA as to the content of the controller's privacy policy, resulting in a violation of Art. 13 GDPR.

In particular, the LSA ruled that the information concerning the right to object under Art. 21(1) GDPR is drafted in a confusing manner which made it more difficult for data subjects to exercise their right to object to processing of their data for direct marketing purposes. As a result, an infringement of Art. 21(4) GDPR was found by the LSA. Finally, the LSA considered

that, as the complainant had the right to request a simplified invoice without being asked for an identification number to be issued, the controller infringed Art. 6(1) GDPR and, consequently, the principle laid down in Art. 5(1)(a) GDPR.

In view of the above, the LSA imposed on the controller an administrative fine of EUR 6,000 for infringements of Art. 5(1) (c), Art. 6(1), Art. 12, Art. 13 and Art. 21 GDPR. The controller was given three months to align its privacy policy with Arts. 12 and 13 GDPR, as well as to stop requesting the customer's tax identification number, unless it obtained valid consent or it is required by law to process this data.

### **LSA: Romanian SA**

**Data subject rights / Right to erasure / Right to be informed / Publicly available data**

Year of decision: 2021

OSS register number: not available yet

The investigation started following a complaint from a Polish citizen claiming that their personal data had been published on the website of the controller without their consent and that they had requested data erasure. The controller, headquartered in Romania, manages online catalogues based on data collected from public databases from various countries in order to facilitate the fast search of information related to over 60 million companies and professionals. The website is available in various versions of European domain names and in the national languages of multiple EU Member States.

According to the controller, the identification elements of the complainant in the controller's online catalogue included the professional name and address, the trade register number, the fiscal attribute and the field of activity, which were all collected from a public database. The controller also indicated

that the deletion option was accessible on the website without the controller being notified. The controller further explained that the complainant's request on the website had not been processed by error and their subsequent email had been sent to spam and not processed on time. Consequently, the controller found out about the request only after the LSA contacted them and immediately took measures to erase the data and inform the complainant.

The LSA found that the controller did not handle the request in accordance with Art. 17 GDPR and did not send a reply within the deadlines provided by Art. 12(3) GDPR. The LSA also recalled that, pursuant to Art. 24 GDPR, the controller is obliged to implement appropriate technical and organisational measures to ensure and be able to demonstrate that the processing is performed in accordance with the GDPR. This includes appropriate and effective measures guaranteeing that all requests received via publicly provided contact details are assessed and handled under the conditions and deadlines provided for in Art. 12 to Art. 22 GDPR.

Furthermore, the LSA concluded that the controller had not provided the data subject with the complete information required under Art. 12 to Art. 14 GDPR, including information regarding the legal basis of the processing. The LSA highlighted that all situations, in which a controller processes information allowing the identification of individuals, even if related to their professional activity, fall within the material scope of the GDPR.

In light of the above, the LSA issued reprimands to the controller. The LSA also imposed corrective measures on the controller: to implement appropriate technical and organisational measures, including appropriate data protection policies; to ensure the lawfulness of the processing in accordance with Arts. 5 and 6 GDPR of personal data that is available in online catalogues; to provide all the necessary information in accordance with Art. 12 to Art. 14 GDPR and to

ensure respect of the data subjects rights, as provided by Art. 15 to Art. 22 GDPR.

### **LSA: Maltese SA**

#### **Restriction of processing / Data subject rights / Debt collection**

Year of decision: 2021

OSS register number: EDPBI:MT:OSS:D:2021:272

In this case, a complainant alleged that the controller obtained his personal data from an unspecified source and was requesting repayment of a loan which the complainant never took. The complainant also stated that he had been a victim of identity theft by a third party and requested to determine how his data had come into the possession of the controller.

In response, the controller stated that it had been informed by the police about the illegal use of the complaint's personal data and had immediately stopped all debt collection activities. The controller had also received a letter from the complainant requiring refraining from processing any personal data of the complainant and to discontinue any communication with regard to the loan. The controller had decided not to reply to this letter based on the understanding that any further communication was undesirable for the complainant. As to the source, from which the personal data had been collected, the controller explained that it had been obtained through a loan application via the website after the applicant's identity had been verified. The controller also informed the LSA that it was subject to legal obligations under which the retention period for personal data related to loan applications and agreements could be up to 10 years.

On the question of determining the source of the complainant's personal data, the LSA noted that the complainant had not

explicitly asked the controller to provide him with information regarding the source of his data. Nevertheless, the controller did provide this information to the LSA. As regards the request to restrict the processing of the complainant's personal data, the LSA found that the controller acknowledged and complied with the complainant's request to restrict the processing of his personal data. Regarding the lack of response by the controller, the LSA noted that the controller violated Art. 12(3) GDPR which lays down an obligation to provide the complainant with information on the action taken on a request under Art. 15 to Art. 22 GDPR, without undue delay and in any event within one month of receipt of the request. As regards the request for erasure, the LSA agreed that the data could not be deleted because processing was necessary to comply with national legislation to which the controller is subject.

The LSA issued a reprimand to the controller.

## **LSA: Norwegian SA**

### **Lawfulness of processing / Performance of contract / Direct marketing / Right to object**

Year of decision: 2021

OSS register number: EDPBI:NO:OSS:D:2021:292

This case involves a complainant who had been receiving direct marketing by email without having the possibility to opt out upon registration of his email address. He had objected to this processing in September 2018, yet he still received a direct marketing email in November 2019. The complainant contacted the DPO of the controller on several occasions, and at times, his requests were answered in more than one month. When he requested the legal basis for the processing of his personal data, which he believed to be consent under Art. 6(1)(a) GDPR, the DPO wrote in response that the legal basis was rather a necessity for the performance of a contract

pursuant to Art. 6(1)(b) GDPR. Later, in another email to the complainant, the DPO stated that the legal basis was Art. 6(1)(f) GDPR for the purpose of marketing the controller's similar products and Art. 6(1)(b) GDPR for the purpose of marketing in relation to the customer benefit program.

The LSA established that there was no designated opt out possibility for marketing from the controller, but it was possible to 'approve' digital marketing via email and SMS on the user's page. As regards the lawfulness of the processing, the LSA reasoned that processing based on contractual performance must be objectively necessary, i.e. the controller should be able to demonstrate how the main subject matter of the specific contract with the data subject cannot be performed without the specific processing of the personal data in question. The processing of personal data for marketing purposes by the controller was not necessary for the performance of the contract related to the provision of a credit card service, and therefore, Art. 6(1)(b) GDPR could not provide the legal basis for the processing. The LSA found that the controller could not retroactively change the legal basis (from contractual performance to legitimate interest) after having commenced with the processing, as this leads to a lack of predictability for the data subject. In any event, a change in the legal basis for processing shall be communicated to the data subjects pursuant to Art. 12 to Art. 14 GDPR.

Further, the LSA found that the controller breached Art. 21(3) GDPR by continuing the processing of the complainant's personal data for direct marketing purposes after his objection to the controller's DPO. The provision of insufficient information on the legal basis of processing and the failure to inform the data subject on his right to object to processing for direct marketing by the controller constituted a breach of Art. 13(1), Art. 12(1) and Art. 21(4) GDPR. Finally, the controller's delays of over a month to respond to the complainant's requests, and without giving him reasons for these delays, constituted a breach of Art. 12(3) GDPR.

The LSA issued a reprimand and ordered the controller to implement measures to ensure that personal data is no longer processed for direct marketing when so requested by data subjects and to ensure that data subject requests under Art. 15 to Art. 22 GDPR are answered within the time limits set in Art. 12(3) GDPR.

## LSA: Swedish SA

### Join controllership / Direct marketing

Year of decision: 2021

OSS register number: EDPBI:SE:OSS:D:2021:236

A complainant stated that a company provided the complainant's email address to a third party for the purpose of sending direct marketing to the complainant without having a legal basis for it. In December 2018, the complainant requested from the third-party access to his data under Art. 15 GDPR, which revealed that the company disclosed the complainant's personal data to the third party. The company stated that this took place in 2017, before the introduction of the GDPR on 25 May 2018 and as such, in 2017, when the complainant's email address was sent to the third party in order to be able to target marketing using the third party's custom audience function. This process was carried out in accordance with the applicable legislation.

In spring 2018, before the introduction of the GDPR on 25 May 2018, the third party changed its terms for the custom audience function and placed the data in quarantine until the company would accept the new terms and conditions of the third party. During this period, the company did not have access to or the possibility to use, modify or delete the personal data. The company approved the third party's new terms in January 2019 and the quarantine personal data was then unlocked by the third party, after which the company deleted the complainant's information.

According to the company, it was only the controller for the transfer of the complainant's personal data to the third party and for any direct marketing that took place before the personal data was quarantined, i.e. before the GDPR began to apply. Furthermore, the company stated that during the period of the GDPR, the company only processed the data subjects' personal data for direct marketing with their prior consent.

The LSA examined whether the company has been a joint controller during the time the personal data was quarantined, i.e. from spring 2018 (before the introduction of the GDPR and when the controller did not approve the third party's conditional changes) until January 2019 (when the personal data was erased). The LSA found that the company transferred the complainant's email address to the third party for the purpose of direct marketing to the complainant. From the moment the personal data was locked by the third party, no direct marketing has been made to the complainant. Since the company did not approve the third party's conditional amendments, it could not continue to process the personal data for the purpose it was transferred to the third party. The company also did not instruct the third party to store the personal data in quarantine. In these circumstances, the purpose of the processing seems to have changed when the third party unilaterally decided to quarantine the complainant's personal data. This indicates that the third party alone determined the purpose and means of processing and that the third party has been solely responsible for the continued processing (storage).

According to the LSA, in this case, it has not been shown that the company had the opportunity to dispose of the data or affect the processing of the data while quarantined. Furthermore, the company has stated that it lacked knowledge of whether the third party has directed direct marketing to the complainant while the personal data was locked. In an overall assessment of the circumstances, the LSA found that

the company cannot be regarded as a joint data controller while the personal data was locked by the third party.

This supervision covers only the company's processing of the complainant's personal data in accordance with the GDPR. The LSA, therefore, found that the investigation in the case did not show that the controller had processed the complainant's personal data in violation of the GDPR. The LSA decided to close the case.

#### 6.1.4. Mutual assistance

The mutual assistance procedure allows SAs to ask for information from other SAs or to request other measures for effective cooperation, such as prior authorisations or investigations.

Mutual assistance can be used for cross-border cases subject to the OSS procedure, either as part of the preliminary phase, to gather the necessary information before drafting a decision or for national cases with a cross-border component.

The IMI enables the use of either informal mutual assistance without any legal deadline (voluntary mutual assistance) or the use of formal mutual assistance. In the latter case, according to the GDPR, the SA from which information has been requested has a legal deadline of one month to reply.

Between 1 January 2021 and 31 December 2021, SAs initiated 243 formal mutual assistance procedures and 2418 voluntary mutual assistance procedures.



#### 6.1.5. Joint operations

The GDPR allows SAs to carry out joint investigations and joint enforcement measures. Similar to the Mutual Assistance procedure, SAs can use joint operations in the context of cross-border cases subject to the OSS procedure, or for national cases with a cross-border component.

In 2021, SAs did not carry out any joint operation.

### 6.2. NATIONAL CASES

SAs have different investigative, advisory and corrective measures at their disposal to ensure entities within their countries apply data protection law correctly and consistently. Corrective measures include the following:

- Issuing warnings to a controller or processor where its intended processing operations are likely to infringe the GDPR;
- Issuing reprimands to a controller or processor where processing operations have infringed the GDPR;
- Ordering the controller or processor to comply with a data subject's request or to bring processing operations into compliance with the GDPR;
- Imposing processing limitations, bans or fines.

#### 6.2.1. Some relevant national cases with exercise of corrective powers

SAs play a key role in safeguarding individuals' data protection rights. They can do this by exercising corrective powers. The EDPB website includes a selection of SA supervisory actions. This section of the Annual Report contains a non-exhaustive list of certain national enforcement actions in different EEA countries carried out outside the OSS cooperation mechanism.

Several cases highlighted a lack of proper technical and organisational measures for processing personal data securely, which led to data breaches. Many other cases revolved around data processing without a data subject's consent. Some significant incidents involved the unlawful processing of special categories of personal data, such as health data. Numerous cases involved data subjects who could not effectively exercise their rights, such as the right of access, the right to erasure and the right to object to a processing act. A great number of cases also include the controller's failure to notify the data subjects of the occurred or the potential risk of data breaches. The entities fined were from both the private and the public sectors.

## 6.2.1.1. Austria

The Austrian SA carried out several investigations and gave a number of fines and warnings during 2021.

On 17 February, the Austrian SA imposed a fine of EUR 4,000,000 on an Austrian bank for failing to ensure that the bank customer data processed as part of an Excel file, which had been unintentionally sent to 227 unauthorised recipients, was encrypted or otherwise protected by an access authorization system that would prevent unauthorised access and unintentional disclosure to third parties.

On 26 July, the Austrian SA issued a fine of EUR 2,000,000 on a data controller that processed data, for a loyalty program, solely based on invalid consent. In particular, it found that the requests for consent from the data controller were designed in such a misleading manner that no valid consent by the data subjects could be assumed. This made the data profiling unlawful, retrospectively for the entire period.

On 28 September, the Österreichische Post was fined EUR 9,500,000 for failing to facilitate the exercise of data subjects' rights. In fact, the controller systematically restricted their

rights by ignoring and not processing inquiries sent by email, which were later disposed of together with the mailbox. The affected data subject had to submit a completely new application through a predefined contact form, regardless of their previously submitted inquiry through email. The contact form also limited the ways in which the data subjects could identify themselves.

## 6.2.1.2. Belgium

The Belgian SA addressed numerous complaints and found violations by data controllers on issues related to, among others, transparency, data subjects' rights, marketing, trading data, smart cameras and COVID-19. This section expands upon a selection of interesting cases.

In January, the Litigation Chamber of the Belgian SA issued a fine of EUR 50,000 and ordered the controller, a company distributing promotional packages, to comply with the GDPR. The decision was made in consideration of the number of data subjects affected, the seriousness of the breach and the nature of the data processed. In particular, it found that the controller did not properly inform the data subjects about the trading of their data and the consent given by them for these data transfers were not valid, as consent was clearly not informed, but also not specific or freely given.

Later in April, the Belgian SA adopted a decision on the responsibility of a controller (a bank) for the abusive usage of the IT system by one of its employees. The controller was fined EUR 100,000 and was ordered to make all employees' access to the database of the Central Individual Credit Register of the Belgian National Bank compliant with Art. 5(1)(f) and Art. 32 GDPR. To achieve such compliance in a transparent and traceable manner, the controller should keep a journal of IT logs.



In December, there were four cases worth highlighting.

The first one revolves around a controller who was sanctioned for not complying with a request to erase personal data in the context of unsolicited direct marketing communication. The Litigation Chamber of the Belgian SA established that the controller's actions amounted to a violation of Art. 12, Art. 14, Art. 15, Art. 17 and Art. 21 GDPR. In addition, it ordered the controller to inform, within 1 month, all data subjects whose personal data had been acquired and further issued a fine of EUR 10,000.

The second case concerned the exercise of the right to be forgotten. A press group refused to delete numerous press articles archived and available on their website that contained personal data of the complainant. Despite the complainant's efforts in arguing for deletion, anonymisation or replacement of his identity with his initials, the Belgian SA dismissed the complaint by indicating that the press publishers were right to refuse the requested deletion.

In the third case, a reprimand was issued against the petition platform Change.org (the controller) for repetitively sending emails. The controller was ordered to communicate, at the first moment of contact with the email recipient, how can the data subjects' rights be exercised more transparently, but also include a link to its privacy policy. In order, to ensure compliance, the controller was ordered to submit evidence of compliance to the Belgian SA.

The fourth case concerned a controller's IT system that did not permit the full enjoyment of the right of correction and also dealt with an issue of conflict of interest of the controller's DPO. The Belgian SA discontinued the proceedings for infringement of Art. 5(1)(d), Art. 16 and Art. 25 GDPR since the controller (a bank) proved that the necessary steps were taken to process the diacritical marks in the names of the clients. However, as the conflict of interest on the part of the

bank's DPO constituted a violation of Art. 38(6) GDPR, the controller was issued a fine of EUR 75,000.

In 2021, the Litigation Chamber of the Belgian SA also handled another interesting case in relation to smart cameras and the use of cookies. It was concluded that there was no infringement pertaining to the setting up of cameras by the controller Westtoer at the Belgian coast to measure the number of visitors during the summer months due to the risks associated with COVID-19. However, the Litigation Chamber reprimanded the controller and ordered to bring certain things (such as the consent for the use of cookies on Westtoer's website, its register of processing activities and its privacy policy) into compliance.

### 6.2.1.3. Bulgaria

In 2021, the Bulgarian SA experienced a continued increase in the number of complaints and actions taken from 2020. Up until 30 September, it issued a total of 408 decisions that addressed complaints from a number of different data subjects and legal entities, state authorities and organizations. Upon reviewing the complaints, the following corrective powers were imposed: one warning, 10 official warnings, three orders for execution of requests of a data subject and 66 orders for administrative penalties. Most violations were made by data controllers processing personal data in the area of courier services, heat accounting, hospitals and other medical institutions, as well as mass video surveillance. This section will cover a selection of cases.

The Bulgarian SA handled a case concerning illegal dissemination of personal data. It concluded a violation of Art. 32(1)(b) GDPR on the side of the controller, the Ministry of Health of the Republic of Bulgaria, and the processor, the liquidator of SBDPLFZR – Raduntsi. The SA issued two penal decrees imposing a "property sanction" on the Ministry of Health in his capacity as personal data controller and a

“penalty” on the liquidator in his capacity as personal data processor.

A public figure filed a complaint to the Bulgarian SA for the improper disclosure of personal information by the controller, a press media website, in a website article. The controller argued that the data had been processed for journalistic purposes. Bearing in mind the public nature of the data subject’s profile, the case required a good balance between the right to protection of privacy and the right to freedom of expression and the right to information. The SA concluded that the publication of the complainant’s date of birth and the full address was not in line with the principle of data minimisation, therefore that information needed to be deleted. Due to the violation of Art. 5(1)(c) GDPR, the SA issued a fine of EUR 2,500 on the controller. The decision of the Bulgarian SA was appealed twice, but the Supreme Administrative Court of Bulgaria finally confirmed and upheld the decision made by the SA.

A complaint has been raised before the Bulgarian SA against the Supreme Administrative Court of Bulgaria after denying a data subject’s access to their assessed written work, which violated Art. 15 GDPR. Furthermore, upon a revision of the controller’s internal rules and the register of processing activities, the SA established that the controller has managed to limit the scope of the concept of personal data.

#### **6.2.1.4. Cyprus**

The Cyprus SA issued multiple fines in 2021. The Cyprus SA carried out these enforcement acts:

- Issued a fine of EUR 925,000 on the controller WS WiSpear Systems Ltd for the collection and storage of Mac Addresses (Media Access Control Address) and IMSIs (International Mobile Subscriber Identity), in breach of GDPR Art. 5(1)(a) GDPR;

- Imposed a fine of EUR 40,000 on the controller APOEL FOOTBALL (PUBLIC) LTD for violating Art. 24(1) and Art. 32(1) GDPR and ordered it to inform potentially affected football fans by the data breach. The SA also issued another fine of EUR 40,000 on the controller OMONOIA FOOTBALL LTD for the violation of Art. 24(1) and Art. 32(1) GDPR and a fine of EUR 25,000 on the processor Hellenic Technical Enterprises Ltd for breaching Art. 28(1) and Art. 32(1) GDPR;
- Issued a EUR 10,000 fine to the Mediterranean Hospital of Cyprus for violation of Art. 31 and Art. 58(1)(a) GDPR due to its disregard of the SA Commissioner’s orders and for avoiding cooperation with the SA.

The Cyprus SA also issued six fines to various controllers for providing unsolicited communication to data subjects, including the following:

- A fine of EUR 12,000 to the Democratic Party;
- A EUR 4,500 fine to the EDEK Social Democrats political movement;

#### **6.2.1.5. Czech Republic**

In 2020, the Czech SA fined a controller CZK 50,000 (EUR 2,000) for publishing personal data of participants in court hearings that were meant to be public in a limited time period. The SA stated that the controller did not have any legal ground to publish the data and highlighted that the right to privacy overrode interest in further data disclosure without considering the individuality of every case. The controller was further ordered to cease the processing of the personal data in a separate proceeding.

#### **6.2.1.6. Denmark**

Unlike in other EEA jurisdictions where the SAs have the authority to issue administrative fines themselves, in Denmark, the Danish SA first investigates a data protection

legal violation and then reports it to the police. The police then investigate whether there are grounds for raising a charge and finally a court decides on a possible fine.

In January, the Danish SA decided that the IT University of Copenhagen did not breach any data protection rules by using a supervision program for online exams. Later in February, the Danish SA handled a case where it decided that the controller Medical Services was not breaching any rules by recording telephone conversations, but it should have not kept the recordings for too long. The controller was ordered to delete all recordings that are more than five years old.

In March, the controller Statens Serum Institut (SSI) was sanctioned with serious criticism for its COVID-19 modelling project. In particular, the Danish SA critiqued SSI for initiating the processing of personal data without adequate risk assessment, impact assessment, consultation with the Danish SA, data processor agreements and appropriate safety measures.

In June, the Danish SA reported Nordborholms Byggeforretning ApS to the police and recommended a fine of approximately EUR 54,000 due to the controller's unlawful disclosure of information about criminal offences of a former employee. In July, the Danish SA reported Medicals Nordic I/S to the police and proposed a fine of approximately EUR 80,000 for treating confidential and health information about citizens in connection with COVID-19 tests, without establishing the necessary security for the processing of the data. Additionally, upon investigation, it was assessed that the infringements were committed intentionally since the controller had not carried out the necessary risk assessments in connection with the processing.

In August, the Danish SA reported the Danish Immigration Service to the police and proposed a fine of approximately EUR 20,000 for failing to meet the requirements for an adequate level of security as per the GDPR.

In September, the Danish SA expressed serious criticism against the municipality of Helsingør for its processing of personal data that used a complex technology in which the data subjects were children and youth, with parts of the processing showing a lack of legal basis. Moreover, the municipality could not demonstrate possession of necessary documentation related to the processing, nor took any adequate organisational and technical measures to ensure the necessary level of security. In the same month, the SA reported Kræftens Bekæmpelse to the police and recommended a fine of approximately EUR 108,000 for the repeated problems with insufficient protection of health data of, among others, cancer patients' health information.

### 6.2.1.7. Estonia

On 30 July, the Estonian SA issued a precept with a penalty payment of EUR 20,000 (per point previously set out) on the controller Register OÜ. It requested the controller to terminate the processing of the data of natural persons on two websites until it meets the necessary data protection requirements.

On 5 August, the Estonian SA issued a reprimand to AS A&P Mets for the unlawful data processing which constituted a violation of the requirements of the GDPR and the Electronic Communications Act. The SA further noted that if the unlawful data processing continues, the SA has the possibility to consider imposing a penalty payment as previously indicated to the controller.

### 6.2.1.8. Finland

In this section, four cases from the Finnish SA's work in connection to data protection violations will be presented.

The Finnish SA handled a case concerning data protection violations connected to parking control fees. The SA issued a reprimand to the controller ParkkiPate for processing personal data in violation of the GDPR and ordered it to act in compliance with the law. In addition, the controller was issued a fine of EUR 75,000 by the sanctions board.

On the basis of GDPR infringements, the SA's sanctions board imposed a fine of EUR 8,500 on a controller for carrying out direct marketing with robocalls without the consent of the call recipients. The Finnish SA decided to permanently prohibit the controller from processing the personal data, gathered based on unlawful consent, for direct marketing.

The sanctions board of the Finnish SA issued a fine of EUR 25,000 on the controller for data protection violations connected to the processing of location data of employees. The employees doing remote work were required to record their working hours in a mobile application that required allowing the use of location data. The SA issued a processing ban on the controller, covering all processing related to location data being or having been collected with the application.

The Finnish SA reprimanded the National Police Board for illegal processing of special categories of personal data with facial recognition software (Clearview AI). Apart from the reprimand, the National Police Board was ordered to notify the data subjects of the personal data breach insofar as their identity could be determined, but to also request from the Clearview AI service the erasure of the data transmitted by the police from its storage platforms.

### 6.2.1.9. France

France handled a number of cases in 2021 where it issued significantly large fines. A selection of cases is presented in this section. On 11 January, the restricted committee of the French SA imposed a fine of EUR 75,000 on the controller, a company specialized in the development of IT solutions for independent food retailers. The French SA noted the controller's inadequacy in taking actions considering the increase of website attacks and the lack of implementation of intermediate measures that could have limited the risk of new data breaches. The SA further emphasised the ineffectiveness of the developed anti-robot tool and observed the possibility that all user accounts were exposed to attacks over a long period of time.

On 20 July, the controller SGAM AG2R LA MONDIALE was fined EUR 1,750,000 for processing operations that violated Art. 5(1)(e), Art. 13 and Art. 14 GDPR. The controller was in breach of Art. 5(1)(e) GDPR since it had not implemented the data retention periods it had defined. The violation of Arts. 13 and 14 GDPR was established based on the non-disclosure of the information regarding the recording of telephone calls and the right to object to being recorded. In addition, the lack of provided information of other data subjects' rights did not allow access to more comprehensive information.

On 26 July, the French SA's restricted committee imposed a fine of EUR 400,000 on MONSANTO for the disregard of its obligations under Art. 14 GDPR in terms of information and Art. 28 GDPR in terms of a contractual framework with a processor. In relation to Art. 14 GDPR, the French SA considered that the creation of contact files by lobbyists for lobbying purposes is not, in itself, illegal. However, the individuals who were listed on such file should have been informed of the existence of the file and consequently, allowed to exercise their right to object to such listing. With respect to Art. 28 GDPR, MONSANTO, as data controller, should have governed the processing carried

out on its behalf by its data processor by a legal act, especially by providing guarantees regarding data security.

On 29 October, the French SA issued a fine of EUR 400,000 on the controller RATP. The SA concluded the existence of a violation of Art. 5(1)(c) and (2) GDPR for the unnecessary data collection on strike days exercised by bus centre agents who were up for promotion. RATP had also breached Art. 5(1)(e) GDPR by failing to limit the duration of storing certain data of staff members, but it has managed to take necessary measures during the proceedings of the case to address this issue. The SA also found that the controller violated Art. 32 GDPR by not implementing appropriate security measures for data processing that can prevent any misuse of the data and guarantee confidentiality.

#### **6.2.1.10. Germany**

Germany has both a national (federal) SA and regional SAs. In 2021, an important case was dealt with by the Hamburg SA in which a fine of EUR 901,388.84 was imposed on the controller Vattenfall Europe Sales GmbH. The SA concluded that the controller breached its transparency obligations under Arts. 12 and 13 GDPR since it did not sufficiently inform the customers about the data comparison. Overall, this affected approximately 500,000 people. The SA further noted that the fine does not affect the question regarding the permissibility of comparison, which is not clearly regulated in the GDPR or any other legislation.

#### **6.2.1.11. Greece**

In a national case before the Hellenic SA, a sports trading company was fined EUR 20,000 for not erasing a complainant's phone number, although being requested to do so. This constituted a violation of Art. 17 GDPR in conjunction with Art. 21(3), Art. 12(3) and Art. 25(1) GDPR since the controller infringed on the data subject's right to erasure and did not ensure a correct procedure of ex-post fulfilment of that right.

The Hellenic SA issued a fine of EUR 15,000 to a company for illegally installing and operating a video surveillance system in the employees' offices and the kitchen of the workplace in breach of Art. 5(1)(a) and (2) GDPR. The company was also ordered to uninstall the cameras and delete any collected material.

An educational centre was issued two fines by the Hellenic SA for data protection violations. First, it imposed a fine of EUR 3,000 for a failure to satisfy the father's right of access to data of his minor child. Later on, the educational centre was fined an additional EUR 5,000 for non-compliance with the order of the Authority to satisfy the complainant's right of access.

In another case, the Hellenic SA issued two fines to the controller Municipal Transportation Company for breaching data protection rules. It fined the controller EUR 5,000 for breaching Art. 12(3) and Art. 15 GDPR by not fulfilling the complainant's right of access to a copy of recorded video material. The second fine amounted to EUR 3,000 as a result of infringement on the principle of proportionality, guaranteed under Art. 5(1)(c) GDPR, when the controller provided the complainant with the service certificate he requested after his dismissal from the company, but added therein that the complainant was fired as a result of a criminal offence.



### 6.2.1.12. Hungary

This section sets out seven pertinent instances in which the Hungarian SA imposed numerous fines for violations of data protection law.

On 29 September 2020, the Hungarian SA handled a case concerning sound recordings of customers at a controller's Customer Service Office. The controller argued that it informed its customers about the sound recordings through the number allocation system, in the general information accessible on its website and the Privacy Statement constituting an annex to its General Terms and Conditions of Contract. The SA concluded that the company did not have an appropriate legal basis for recording its customers and failed to take into consideration the customers' right to object. It further noted that in light of the absence of identification and clarity, the sound recording by the controller failed to comply with the principle of purpose limitation. The SA also found a breach of the principle of data minimisation since recordings were conducted throughout the entire process of administering personal cases and a breach of the principle of transparency due to the provided information by the controller which was deficient and comprised of misleading statements.

On 9 December 2020, a controller of the financial service sector was fined EUR 5,448 by the Hungarian SA. The decision was based on an infringement of Art. 32(1) GDPR since the controller did not implement sufficient data security measures for the processing of personal financial data.

In another case on the same day, the Hungarian SA established violations of Art. 25, Art. 32 and Art. 34 GDPR by a travel agency since it had entrusted the design of the website to an inadequate data processor, could not guarantee the security of the personal data processed and did not inform the data subjects about a high-risk data breach. In addition, the processor also violated Art. 32 GDPR since it failed to

implement appropriate security checks on the website and acted with a high degree of negligence towards the website's development. Consequently, the controller was fined EUR 55,000 and the processor was fined EUR 1,375.

On 16 December 2020, the Hungarian SA issued a fine of EUR 98,600 on the controller, a bank, for breaching Art. 5(1) (c), Art. 6, Art. 9 and Art. 12(1) GDPR. The SA found that the bank, when processing copies of pregnancy care books, has processed some personal and special category personal data that was neither suitable, nor necessary for the purpose of the processing. The bank also did not have any legal basis for processing part of the data and it failed to provide unambiguous and transparent information on the processing of the personal data included in the copies of the pregnancy care books. Apart from the issued fine, the SA ordered the bank to annihilate the copies of the pregnancy care books and to transform the information provided on its processing.

On 24 March 2021, the Hungarian SA concluded the existence of several data protection violations by the Budapest Capitol's Government Office's XI. District Office. The infringement of Art. 32(1)(a), (b) and (2) GDPR was based on the insufficient application of data security measures by the controller regarding the transfer of medical data, which resulted in the possibility of causing a high-risk data breach. The controller violated Art. 33(1) GDPR when it did not consider it necessary to report the high-risk personal data breach to the Hungarian SA since it did not carry out the risk analysis properly. The violation of Art. 34(1) GDPR occurred since the controller did not communicate the high-risk data breach to the data subjects. A fine of HUF 10,000,000 (approximately EUR 28,000) was imposed on the controller.

On 18 June 2021, the Hungarian SA imposed a fine of EUR 13,705 and ordered the erasure of the data processed to an electronic media content service provider for multiple GDPR infringements. In this case, the controller published

personal and health data of a minor, making him identifiable, although that was not necessary for achieving the purpose of broadcasting news. Furthermore, the controller published the data without any legal basis since it did not acquire consent and it disregarded the preliminary objection of providing consent by the data subject's relative. The SA also found that the controller acted contrary to the principle of fair data processing by broadcasting news about a data subject who was physically incapacitated and therefore unable to express intent to consent or object to such processing.

On 27 October 2021, the Hungarian SA handled a case in which the data subject was not informed by the controller or processor of the data processing. In addition, the SA concluded that the processor did not have any legal basis for processing data that fell outside the scope of essential data for complaint management purposes. Consequently, the SA determined the existence of numerous violations of the GDPR, imposed a fine and requested a modification of the data processing.

#### **6.2.1.13. Iceland**

The Icelandic SA dealt with a number of cases, with some of them focusing on COVID-19.

On 15 June, the Icelandic SA issued a fine of EUR 34,000 on the controller Huppuís ehf., a company running ice cream parlours. The SA found that the processing of the employee's personal data via video surveillance camera installed in an employee area was not lawful, fair or transparent, nor adequate, relevant and limited to what was necessary in relation to the purposes for which the data was processed.

On 23 November, the Icelandic SA concluded that the conducted data protection impact assessment (DPIA) concerning the move of the microbiology department of the controller, the National University Hospital of Iceland, to the sub-processor, the company Decode Genetics, did not fulfil

the GDPR requirements. Nevertheless, the SA established that nothing indicated non-compliance with the GDPR in relation to the security of personal data processed on the premises of Decode Genetics.

On the same day, 23 November, the Icelandic SA also decided on another case involving the same actors, the National University Hospital of Iceland and the company Decode Genetics. In this case, the SA determined that the processing of personal data by the two actors was not in compliance with the GDPR due to a lack of approval from the National Bioethics Committee. However, bearing in mind the urgency and importance of the work surrounding COVID-19, the SA decided not to issue fines in this case.

The Icelandic SA handled a third case revolving around the same actors on 23 November. In this case, the controller was the National Chief Epidemiologist who was ordered to update the processing agreement with the National University Hospital of Iceland so that the agreement would be in line with Art. 28 GDPR. Comparable to the previous case, in this case the SA also did not issue fines in light of the urgency and importance of the work surrounding COVID-19.

One day after, on 24 November, the Icelandic SA imposed a fine of ISK 7,500,000 (approximately EUR 50,800) on the controller, the Ministry of Industries and Innovation of Iceland, and imposed a fine of ISK 4,000,000 (approximately EUR 27,100) on the processor, the company YAY ehf. The case revolved around a digital gift card app that unlawfully and unnecessarily collected substantial amounts of personal data and acquired access rights to the user's mobile devices.

The SA determined that consent was given by the app users and there was a lack of information transparency. In addition, the controller and the processor had not ensured the appropriate security of the personal data, had not made a processing agreement and had not implemented data

protection by design and by default that could have ensured data minimisation.

### 6.2.1.14. Ireland

The Irish SA, on its own volition, started an inquiry into the Department of Employment Affairs and Social Protection after receiving a complaint from Digital Rights Ireland. The SA concluded no infringement of Art. 38(1) GDPR since the Department involved their DPO properly and in a timely manner in the Department's amendment of its Privacy Statement. No violation of Art. 38(3) GDPR was either found because the Department did not provide any instructions to the DPO regarding the exercise of their tasks contrary to the GDPR.

The Irish SA imposed a fine of EUR 90,000 on the controller, the Irish Credit Bureau DAC (ICB). The ICB violated Art. 25(1) GDPR by failing to implement appropriate technical and organisational measures designed to implement the principle of accuracy effectively and to integrate the necessary safeguards into the processing. A violation of Art. 5(2) and Art. 24(1) GDPR was also established for the ICB's failure to demonstrate compliance with its obligation to undertake appropriate testing of proposed changes to its database. The ICB was issued a reprimand as a result of the committed violations.

In another case, The Irish SA reprimanded and imposed a fine of EUR 1,500 to the controller, Men Overcoming Violence (MOVE) for infringing upon Art. 5(1)(f) and Art. 32(1) GDPR. The SA decided that MOVE failed to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented by its processing by means of recording group sessions on SD Cards containing participants' and facilitators' personal data. The controller was ordered to bring its processing into GDPR compliance.

### 6.2.1.15. Italy

In January, the Italian SA concluded various violations by TikTok in relation to poor attention to the protection of minors on account of the easy circumvention of its age gating mechanism, the distribution of unclear information to users and the poor adherence to privacy requirements by the application's default settings. TikTok was ordered to implement appropriate access limitation measures for minors (below the age of 14) and was prohibited from further processing personal data of users whose age can't be verified.

In February, a case concerning data of applications for a COVID-related bonus was handled by the Italian SA in which a EUR 300,000 fine was issued to the National social security agency (INPS). The SA concluded that the processing by INPS was unlawful. INPS was ordered to erase unnecessary data and carry out an appropriate DPIA.

In April, the Italian SA did not issue a favourable opinion on the use of facial recognition technology through the SARI Real Time system to support law enforcement activities of the controller, the Italian Ministry of the Interior. The SA concluded a lack of legal basis to legitimise the automated processing of biometric data for facial recognition in security applications, particularly because it will enable a mass/blanket surveillance.

In June, the Italian SA issued several corrective measures and a fine of EUR 2,600,000 on the controller Foodinho s.r.l. for several infringements of the GDPR and national law provisions. The corrective measures focused on issues such as transparency, data processing, DPIA, data storage, fairness and accuracy of an algorithm that avoids discrimination, data minimisation, employment and work surveillance.

In the same month, the Italian SA determined that the configuration of the ‘IO’ application of the controller PagoPA Spa, infringed on the GDPR. The controller made commitments to minimise the excessive data collection and transfer to third countries and to implement corrective measures that would remedy the infringements found. As a consequence, the Italian SA decided to lift the previously imposed temporary limitation on the processing of personal data via the ‘IO’ app.

In July, the Italian SA imposed a fine of EUR 2,500,000 on the controller Deliveroo Italy s.r.l. for the poor transparency in using algorithms and the disproportionate collection of employees’ data. The SA also issued numerous corrective measures concerning issues such as transparency, processing records, DPIA, data storage, data safeguards, fundamental freedoms and legitimate interests, fairness and accuracy of an algorithm that avoids discrimination, data minimisation, employment and work surveillance.

Later in September, the Italian SA reprimanded a real estate agency for exchanging information with a data subject on LinkedIn that was contrary to the platform’s Terms of Service. The SA determined that the processing was unlawful and ordered the real estate agency to take suitable organisational measures. Nonetheless, the SA imposed a fine of EUR 5,000 on the controller for its failure to reply to the SA’s repeated requests for information.

In the same month, the Italian SA ordered Sky Italia to pay a fine of over EUR 3,200,000 and banned any further processing for promotional purposes of telephone subscribers’ data the company had obtained from other entities. Sky Italia was also ordered to make a certified email account that will facilitate opt-out requests by data subjects and to appoint all the entities that perform promotional activities on its behalf as data processors whilst Sky, as a controller, supervises the activities of the processors and verify the proper management of users’ information. Interestingly, the Italian SA noted that

the calculation of the fine took into account the gravity of the violations that were grounded in “systematic” practices at a corporate level.

### 6.2.1.16. Latvia

On 14 January, the Latvian SA impose a fine of EUR 65,000 on a data re-user for ensuring public access to data even after the applicable regulatory enactments required to restrict access to such data.

On 14 May, the Latvian SA issued a fine of EUR 100,000 against an online retailer that carried out processing of personal data to identify a natural person without legal basis. The controller was ordered to delete the personal data – copies of imagines of user’s documents – from its website. The decision has been appealed and is still pending.

### 6.2.1.17. Liechtenstein

A private insurance company was found in violation of Art. 6(1)(a), Art. 7 and Art. 13 GDPR for unlawfully obtaining and processing personal data of data subjects. The company was banned from processing the data and was ordered to erase the collected data.

A Swiss company, acting as a controller, was ordered to erase personal data consisting of unlawfully recorded phone calls in Liechtenstein. Even though the controller is established in Switzerland, the SA concluded an infringement of Art. 6(1) GDPR since no consent was obtained from the EEA nationals.

### 6.2.1.18. Lithuania

The Lithuanian SA handled a number of cases in 2021. A selection of those cases is presented in this section.

Upon a conducted investigation, the Lithuanian SA imposed a fine of EUR 12,000 to the National Public Health Centre (NPHC) and a fine of EUR 3,000 to the developer of the application UAB “IT sprendimai sėkmei” (the Company). The two entities acted as joint controllers who processed personal data intentionally, to a large extent, illegally, systematically, without providing technical and organisational means to demonstrate GDPR compliancy while conducting such processing, and they also processed special category personal data.

The Lithuanian SA issued a fine of EUR 15,000 to the State Enterprise Centre of Registers for infringements of Art. 32(1) (b) and (c) GDPR. The controller in this case failed to ensure the ongoing integrity, availability and resilience of processing systems and services, but also failed to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

A case before the Lithuanian SA concerned the processing of biometric personal data in a sports club that resulted in a EUR 20,000 fine for the controller, VS FITNESS UAB. The controller was deemed in violation of numerous GDPR provisions for processing biometric data without the voluntary consent of the data subjects and its failure to ensure other requirements for the valid consent, the unsuitable implementation of the data subjects' right to be informed of data processing, the failure to maintain records of activities and not conducting a DPIA.

One of the cross-border cases before the Lithuanian SA involved the company Prime Leasing UAB, an operator of the short-term car rental platform CityBee, that was fined EUR 110,000 for breach of Art. 32(1)(a), (b) and (d) GDPR. The violation was mainly grounded on the fact that the company did not ensure the security of the processing of personal data of data subjects.

### 6.2.1.19. The Netherlands

In 2020 and 2021, the Dutch SA imposed multiple fines for GDPR violations. Most of the fines were imposed because of serious breaches of data subjects' rights. Selected cases are listed here:

- In March 2020, the maintenance company CP&A B.V. was fined EUR 15,000 for violations committed when processing the health data of sick employees. The company maintained a register of the causes of sick leave, which resulted in processing more health data than legally permitted. Moreover, this register was accessible online and not adequately secured. CP&A has now ended this practice;
- In June 2020, the Dutch SA fined PVV Overijssel an amount of EUR 7,500 for failing to report a data breach to the SA within the applicable time limit – within 72 hours of becoming aware of the data breach;
- In November 2020, the Dutch SA determined a fine of EUR 440,000 for the Amsterdam-based hospital OLVG for its inadequate protection of patients' medical records. The SA established that OLVG did not implement sufficient safeguards to prevent unauthorised access to the records, it did not carry out proper checks of who accessed which records and did not address problems pertaining to the information systems security. Consequently, OLVG worked on the required improvements;
- In March 2021, the Dutch SA issued a fine of EUR 600,000 to the municipality of Enschede for using Wi-Fi tracking in the city centre in a way that is prohibited. Following the intervention by the SA, the municipality stopped such data tracking on 1 May 2020;
- In April 2021, the Dutch SA imposed a fine of EUR 750,000 on TikTok for infringing on young children's privacy. TikTok lodged an objection to the fine. During the course of the investigation, TikTok established operations in Ireland.

- As a result, the Dutch SA transferred other results of the investigation to the Irish SA, which will proceed with the investigation on TikTok's processing operations;
- A month later, in May, the Dutch SA imposed a EUR 450,000 fine on the Employee Insurance Agency (UWV) for the poor security when sending group messages via the "Mijn Werkmap" section of its website, a personal environment in which job seekers can interact with the UWV. The website has suffered multiple data breaches that involved personal and health data of more than 15,000 data subjects;
  - In June 2021, the Dutch SA issued a fine of EUR 12,000 to an orthodontic practice for allowing new patients to register on an unsecured website. This could have led to an unwanted third-party breach of patients' sensitive personal data, such as their citizen service number;
  - In December 2021, the Dutch SA imposed a EUR 2,750,000 fine on the Dutch Tax Administration because for many years it processed data on the dual nationality of childcare benefit applicants in an unlawful, discriminatory and improper manner.

#### **6.2.1.20. Norway**

The Norwegian SA issued multiple fines in 2021. The Norwegian SA carried out the following actions:

- Imposed a fine of EUR 15,000 on the controller Dragefossen AS for live streaming CCTV surveillance recordings of data subjects that were in no way, personally or their activities, connected to the controller;
- Issued a fine of approximately EUR 500,000 to the Norwegian toll company Ferde AS for failing to establish a data processing agreement, to carry out a risk assessment and its lack of legal basis for the processing of personal data about motorists in China;

- Imposed a fine of EUR 100,000 to the controller Innovation Norway for lacking a legal basis of processing personal and financial data in relation to credit rating;
- Imposed a fine of EUR 125,000 to the controller Norwegian Confederation of Sport for inadequate testing involving personal data. The controller did not have a legal basis for processing the data and overall breached the principles of legality, data minimisation and confidentiality;
- Ordered the company Cyberbook AS to implement written procedures for access to the email inboxes of employees and former employees, but also imposed a EUR 20,000 fine for the unlawful automated forwarding of the employee's personal email address to the company;
- Ordered the Oslo University Hospital to amend data processing agreements and therefore ensure the correct handling of the hospital's duties and the protection of patients' rights;
- Issued a fine of approximately EUR 6,500,000 to Grindr LLC for disclosing user data to third parties for behavioural advertisement without a legal basis. The SA concluded that the purported consents that were collected for sharing personal data with advertising partners were not valid. Furthermore, Grindr failed to properly communicate the sharing of personal data to its users. Notably, the SA considered that the sensitive nature of the shared data – belonging to a sexual minority – makes the data a special category data that merits particular protection under the GDPR.

#### **6.2.1.21. Poland**

The Polish SA handled several cases in 2021. One violation that was consistently addressed by the SA was the controllers' failure to notify personal data breaches to the SA. This can be observed in some of the cases presented in this section.

On 11 January, the Polish SA imposed a EUR 30,000 fine on the controller ENEA S.A. for failing to notify a personal data breach once personal data has been accidentally shared with an unauthorised recipient of such data. The breach consisted of a shared email that had an unencrypted, non-password protected attachment containing personal data of several hundred people.

On 11 February, the Polish SA issued a fine of EUR 22,000 to the National School of Judiciary and Public Prosecution (KSSIP) for failing to fulfil its obligations as a controller. While the processor was found to be in compliance with the GDPR rules, the controller breached the confidentiality of data subjects by failing to conduct an analysis of whether it was exposing personal data stored in a database that was shared with the processor.

On 19 March, the Polish SA issued a fine of EUR 5,000 to the company Funeda Sp. z o.o. for its failure to cooperate with the SA, in particular the impediment of access to necessary information.

On 22 April, the controller Cyfrowy Polsat S.A. was fined EUR 250,000 for the lack of implementation of adequate organizational and technical measures for detecting data breaches that should result in the prompt notification to data subject of the risk associated with potential identity theft.

A few days later, on 27 April, the company PNP S.A. was fined EUR 5,000 for violating its obligation of providing access to information to the Polish SA, especially information that was necessary to address the merits of the case.

On 8 June, the Polish SA imposed a fine of EUR 22,000 on the controller P4 Sp. z o.o. for its failure to notify the SA of personal data breaches. The controller did not manage to meet the notification deadline due to employees' errors when dispatching data breach notifications to data subjects through

postal service – a method of notification that was persistently held on to by the controller, although having the opportunity to dispatch electronic notifications.

On 21 June, the Polish SA imposed a fine of EUR 35 000 on the company ERGO Hestia S.A. for failing to notify the SA of a security breach when personal data was made available to an unauthorised recipient that was considered to be untrusted.

On 14 October, the bank Millennium was fined EUR 80,000 for its failure to notify a personal data breach to the SA and also for not communicating it to the data subjects. Consequently, in line with Art. 34(2) GDPR, the bank was ordered to communicate the data breach to the persons affected by it.

### 6.2.1.22. Romania

In October, the Romanian SA issued a reprimand and remediation measures against Cluj-Napoca City for violation of Art. 15(3) and Art. 12(3) and (4) GDPR. The remediation measures consisted of implementing an internal procedure for processing requests submitted by data subjects based on the GDPR, the observance of the applicable provisions regarding the assessment and handling without delay of these requests and communication of answers to the data subjects within the legal deadlines, but also conducting regular personnel training in relation to this.

In April, the controller World Class România S.A. was sanctioned with a EUR 2,000 fine for the violation of Art. 32 GDPR concerning the insufficient security of the processing of personal data. Additionally, the SA issued a corrective measure that ordered the controller to ensure GDPR compliance of the processing (within 30 days of communicating the SA's decision) by implementing appropriate technical and organisational measures in case of remote transmission of the personal data, but also to conduct regular personnel training in respect to this.

In the same month, the controller Telekom Romania Communications S.A. was reprimanded for violation of Art. 6 GDPR since it processed personal data for marketing purposes without a legal basis. The controller was also fined EUR 2,000 for violation of Art. 21 GDPR since it had contacted by phone a data subject, who had previously exercised their right to object.

Later in October, the Romanian SA imposed a fine of EUR 1,000 on the controller IKEA ROMÂNIA SA for infringing on Art. 32(1)(b) and (2) GDPR when a data breach occurred that resulted in compromising the data confidentiality of 114 Ikea Family members.

In November, the Romanian SA took several corrective measures against UAT Municipiul Constanța for possible breach of the data minimisation principle, guaranteed under Art. 5(1)(c) GDPR. The measures consisted of a reprimand for violating Art. 5(1)(c) GDPR and an order to take necessary measures to observe the data minimisation principle in relation to issuance of car access permits for its residents, including through the amendment of the Local Council Decision regarding this processing.

### 6.2.1.23. Slovenia

The Slovenian SA handled several cases in 2020 and 2021. A few cases of particular importance are presented in this section.

The controller National Institute of Public Health was ordered to provide clear, accurate and reliable information on registration for vaccination per Art. 13 GDPR. As a result, the controller informed the data subjects about its function as a data controller, the purpose of data processing, the legal basis, the storage period and the data subject rights.

The Slovenian SA determined that a controller unlawfully monitored work areas through video surveillance. As a result, the controller was ordered to remove the surveillance cameras, with a few exceptions (e.g., the warehouse). The SA also found that the controller failed to ensure traceability of the data processing since it did not keep data records.

The Slovenian SA dismissed a complaint of a data subject that requested the erasure of his personal information from the Baptismal Register of a parish of the Roman Catholic Church. The SA concluded that the right to erasure, guaranteed under Art. 17 GDPR, does not enable an individual to have their personal data erased from the register. The complainant challenged the decision before the national justice system, but nonetheless, the Slovenian Administrative Court upheld the decision of the SA.

The Slovenian SA decided to dismiss a complaint of a patient to rectify a medical report. The SA elaborated that this right enables data subjects to rectify data that is not accurate, while that was not the situation in the case at hand. Concerning the principle of accuracy, the SA stated that the controller is processing accurate personal data of the individual, particularly considering the amendment of the initial medical report that contains additional text, while not deleting previously written text.

A decision of the Slovenian SA determined that a restaurant is not allowed to monitor the movements of individuals across the restaurant through video surveillance. The SA stressed that the safety in the restaurant can be achieved by less privacy intrusive measures, such as monitoring only specific areas like the cash register and the entry. In addition, the SA emphasised that the video surveillance should not be managed by the work supervisors, but rather by security officers.

A series of cases concerning positive infections of the COVID-19 virus resulted in infringements of various GDPR rules. The Slovenian SA found that one state authority violated Art. 5(1) (c) GDPR when informing other employees about co-workers who tested positive to the COVID-19 virus. Moreover, in all three cases, the controller did not inform the employees, who were COVID-19 positive, about the processing of their data, which resulted in the violation of Art. 13 GDPR. In one of the cases, the state authority was issued a fine of EUR 830 and an administration fee in the amount of EUR 83 for processing personal data of an employee without their consent or determination for such processing.

#### **6.2.1.24. Spain**

The Spanish SA issued a number of comparable fines in late 2020 and throughout 2021. The Spanish SA carried out these actions:

- Imposed a fine of EUR 500,00 on the controller EDP ENERGIA, S.A.U. for violating Art. 25 GDPR by not adopting appropriate technical and organisational measures for processing personal data. The controller was also fined EUR 1,000,000 for violating Art. 13 GDPR since it did not adequately provide information to data subjects;
- Issued multiple fines that together amount to more than EUR 8,000,000 (highest fine amount issued by the SA) to the controller Vodafone España, S.A.U. In particular, it imposed a fine of EUR 4,000,000 for infringement of Art. 28 GDPR, a fine of EUR 2,000,000 for infringement of Art. 44 GDPR and two fines in the amount of EUR 2,000,000 and EUR 150,000 for violation of two national laws – General Telecommunications Law and Electronic Commerce Law. Apart from this, the SA also ordered the controller to bring its processing operations into compliance with Art. 17, Art. 21, Art. 24, Art. 28 and Art. 44 to Art. 49 GDPR within six months of the adoption of the decision;
- Imposed a fine of EUR 2,520,000 on MERCADONA, S.A. for the use of a non-legitimised facial recognition system in supermarkets, as well as for lack of transparency, excessive use of personal data, lack of privacy by design and poor impact assessment;
- Issued to the controller EDP ENERGÍA, S.A.U. a fine of EUR 500,000 for violation of Art. 25 GDPR and a fine of EUR 1,000,000 for violation of Art. 13 GDPR;
- Decided to close a case due to the non-infringement of the GDPR. The SA determined that medical data of patients belong to the hospital, the controller, and not to the doctor who treated the patients while working at the hospital;
- Issued a fine of EUR 1,500 to a natural person for posting photographs and notes of sexual content of their partner on a website without the consent of the partner;
- Imposed a total fine of EUR 6,000,000 on CAIXABANK, S.A., for unlawfully processing clients' personal data (in the amount of EUR 4,000,000) and not providing sufficient information regarding the processing of personal data (EUR 2,000,000). Apart from the issued fine, the Spanish SA ordered CAIXABANK to bring its processing operations into compliance with Art. 6, Art. 13 and Art. 14 GDPR within six months of the adoption of the decision;
- Issued a fine of EUR 3,000,000 to the controller CAIXABANK PAYMENTS & CONSUMER EFC, EP, S.A.U. for lack of specific and informed consent regarding profiling for commercial purposes. In addition, the controller was ordered to bring its processing operations in compliance with the GDPR within six months of the adoption of the decision.

#### **6.2.1.25. Sweden**

In 2021, the Swedish SA conducted numerous enforcement measures for violations of the GDPR, some of which

concerned Swedish national authorities. This is illustrated in the cases outlined here.

On 10 February, the Swedish Police Authority was fined EUR 250,000 for breaching the Criminal Data Act (which implements the EU Law Enforcement Directive 2016/680) by using the biometric data tracking application Clearview AI in its operational activities. The Police were ordered to ensure the erasure of data that was transferred to Clearview AI, to inform affected data subjects that their data had been processed by Clearview AI and to conduct personnel training and education in respect to avoiding similar future processing of personal data that is unlawful. The Police decided to appear the decision, which is now to be settled by the Swedish Administrative Court of Appeal.

On 7 June, the Swedish SA issued multiple fines in a case concerning the unprotected web availability of recorded phone calls in relation to medical consultations. The SA imposed a fine of EUR 1,200,000 on the controller Medhelp for its failure to take appropriate security measures, for the lack of provided information to data subjects and for breaching certain provisions of the Swedish health and medical care legislation. The SA imposed a EUR 50,000 fine on Voice Integrate for failing to take appropriate and sufficient security measures to protect phone calls handled on behalf of Medhelp. In addition, the SA issued EUR 50,000 fine on three regional authorities for not providing sufficient information to the data subjects seeking medical care through the service. The decisions of the SA have been appealed and are to be settled by the Swedish Administrative Court of Appeal.

On 9 June, the Swedish SA issued a fine of EUR 34,000 against the Executive Board of the Rescue Service in Östra Skaraborg (Rescue Service). While the SA established that the Rescue Service has compelling reasons for its camera surveillance, it should limit the recording to events when the alarm is activated and should mask areas where firefighters change

clothes in order to capture only necessary information. The Rescue Service has stopped the camera surveillance.

On 21 June, the Swedish SA imposed a EUR 15,500,000 fine to the public transport operator Storstockholms Lokaltrafik (SL) for the infringements of Art. 5, Art. 6 and Art. 13 GDPR. The SA concluded that the authority needs to reduce the pre-recording time on the body-worn cameras for threat prevention to 15 seconds. It also found that the technology should not be used for the identification of passengers without tickets and added that still images and soundless recordings are sufficient for the purpose of threat prevention. The controller also failed to adequately inform about the camera surveillance, in particular that, apart from video, sound was also recorded.

### 6.3. SA BUDGET AND STAFF

The EDPB received a request from the Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) of the European Parliament to share some statistics on resources made available by Member States to the SA from the EEA and on enforcement actions by the SAs. The EDPB already gathered similar information in the past in the context of a 2019 Report about the GDPR implementation made at the request of the LIBE Committee and the contribution of the GDPR evaluation made in 2020 at the request of the European Commission.

On 5 August 2021, the EDPB published an “[Overview of the resources made available by Member States to the Data Protection Authorities and on enforcement actions by the Data Protection Authorities](#)”. The vast majority of SAs (22) explicitly stated that their allocated budget is not sufficient for carrying out the work activities. Based on the information from 29 SAs from EEA countries before August 2021, six SAs even faced a budgetary decrease in comparison to their 2020 budget.

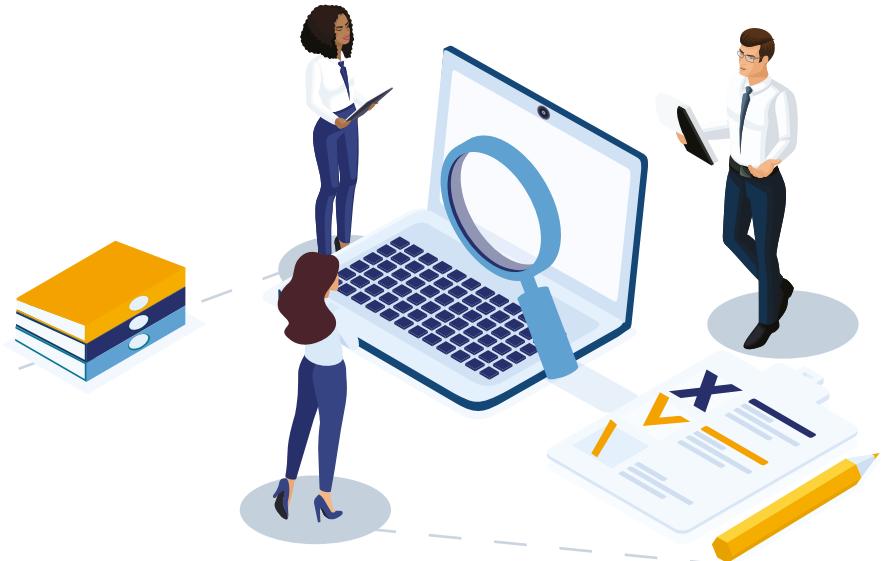
In respect to SAs' human resources, a vast majority of SAs (22) underlined the fact that they do not have enough human resources to face their workload. Ten SAs did not experience any change in their staff numbers, while six SAs saw a decrease in employees in 2021, in comparison to 2020.

The document providing the overview of the SAs' resources also demonstrates that, across the majority of the SAs, a greater number of staff usually works on national enforcement cases in comparison to cross-border cases.

In its contribution to the evaluation of the GDPR adopted in 2020, the EDPB stressed that the effective application of the powers and tasks attributed by the GDPR to SAs is largely dependent on the resources available to them.



## 7



## COORDINATED SUPERVISION COMMITTEE OF THE LARGE EU INFORMATION SYSTEMS AND OF EU BODIES, OFFICES AND AGENCIES

In accordance with Art. 62 of Regulation 2018/1725, the national Supervisory Authorities (SAs) and the European Data Protection Supervisor (EDPS) shall cooperate actively to ensure effective supervision of large-scale IT systems and of EU bodies, offices and agencies. For this purpose, they shall meet at least twice per year within the framework of the EDPB. Additionally, several legal acts on large-scale IT systems and EU agencies refer to this model of coordinated supervision.

To ensure the consistency of supervision efforts on both levels, all SAs involved, including the EDPS, used to cooperate through Supervision Coordination Groups (SCGs).<sup>4</sup> Each of these groups was dedicated to a specific EU database. Since December 2018, Regulation 2018/1725 has provided for a

single model of coordinated supervision for large-scale EU IT systems and agencies within the framework of the EDPB. This replaces the current system of individual SCGs. The new model does not apply to all EU information systems and agencies at once, but progressively, according to when the revised version of the establishing act of each EU information system and agency becomes applicable.

In December 2019, the Coordinated Supervision Committee (CSC) was formally established within the EDPB. It brings together the SAs of each EU Member State and the EDPS, as well as SAs of non-EU Members of the Schengen Area where provided for in EU law.

The CSC's tasks include, among others, supporting SAs in carrying out audits and inspections; working on the interpretation or application of the relevant EU legal act; studying problems within the exercise of independent supervision or within the exercise of data subject rights; drawing up harmonised proposals for solutions; and promoting awareness of data protection rights.

Participation in the CSC meetings can occur under various arrangements, depending on the IT system, body, office or agency for which supervision is taking place, as well as the respective EU legal act. As [announced](#) in December 2020, during its third plenary meeting, the CSC elected Clara Guerra from the Portuguese SA to succeed Giuseppe Busia as its new Coordinator for a term of two years. Sebastian Hümmeler from the German Federal SA currently holds the position of Deputy Coordinator.

Pursuant to Art. 62 of Regulation 2018/1725, the following EU large-scale IT systems, bodies, offices and agencies currently fall under the CSC's scope:

### **Internal Market:**

- Internal Market Information System (IMI), which allows the exchange of information between public authorities involved in the practical implementation of EU law.

### **Police and Judicial Cooperation:**

- Eurojust, the agency responsible for judicial cooperation in criminal matters among EU Member States;
- European Public Prosecutor Office (EPPO), the prosecution agency responsible for investigating, prosecuting and bringing to judgment crimes against the EU budget.

In the future, all coordinated supervision of large EU information systems, bodies, offices and agencies will gradually be moved to the CSC, including:

### **Border, Asylum and Migration:**

- Schengen Information System (SIS), ensuring border control cooperation (expected no later than June 2022);
- Entry Exit System (EES), which registers entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Schengen States (expected before the end of 2022);
- European Travel Information and Authorisation System (ETIAS), which tracks visitors from countries who do not need a visa to enter the Schengen Zone (expected in May 2023);
- Visa Information System (VIS), connecting consulates in non-EU countries and all external border-crossing points of Schengen States (expected by the end of 2023);
- Eurodac, which compares fingerprints of asylum applicants to see if they have previously applied for asylum or entered the EU irregularly via another Member State (expected in 2022);
- Customs Information System (CIS), which is an automated information system that assists EU State administrative authorities in preventing, investigating and prosecuting operations that are in breach of customs or agricultural legislation.

### **Police and Judicial Cooperation:**

- European Criminal Records Information System on third country nationals (ECRIS-TCN), which allows EU Member State authorities to identify which other Member States hold criminal records on third country nationals or stateless persons being checked (expected for 2022);
- Europol, the EU's law enforcement agency (expected in 2022);
- Schengen Information System (SIS) (see above, as this system also fall under Police and Judicial cooperation).

- <sup>4</sup>. In the past, four SCGs were created for the following systems: Schengen, Visa and Customs Information Systems, as well as for Eurodac.



# 8



## ANNEXES

### 8.1. GENERAL GUIDANCE ADOPTED IN 2021

- Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications
- Guidelines 07/2020 on the concepts of controller and processor in the GDPR
- Guidelines 08/2020 on the targeting of social media users
- Guidelines 09/2020 on relevant and reasoned objection under Regulation 2016/679
- Guidelines 10/2020 on restrictions under Art. 23 GDPR
- Guidelines 01/2021 on examples regarding data breach notification

- Guidelines 02/2021 on virtual voice assistants
- Guidelines 03/2021 on the application of Art. 65(1)(a) GDPR
- Guidelines 04/2021 on codes of conduct as tools for transfers
- Guidelines 05/2021 on the interplay between the application of Art. 3 and the provisions on international transfers as per Chapter V of the GDPR
- Guidance on certification criteria assessment (Addendum to Guidelines 1/2018 on certification and identifying certification criteria in accordance with Arts. 42 and 43 of the Regulation)
- Recommendations 01/2020 on measures that supplement

- transfer tools to ensure compliance with the EU level of protection of personal data
- Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive
  - Recommendations 02/2021 on the legal basis for the storage of credit card data for the sole purpose of facilitating further online transactions
- ## 8.2. CONSISTENCY OPINIONS AND DECISIONS ADOPTED IN 2021
- Opinion 01/2021 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of Saxo Bank Group
  - Opinion 02/2021 on the draft decision of the Swedish Supervisory Authority regarding the Controller Binding Corporate Rules of Elanders Group
  - Opinion 03/2021 on the draft decision of the Belgian Supervisory Authority regarding the Controller Binding Corporate Rules of BDO
  - Opinion 04/2021 on the draft decision of the Belgian Supervisory Authority regarding the Processor Binding Corporate Rules of BDO
  - Opinion 05/2021 on the draft Administrative Arrangement for the transfer of personal data between the Haut Conseil du Commissariat aux Comptes (H3C) and the Public Company Accounting Oversight Board (PCAOB)
  - Opinion 06/2021 on the draft decision of the Spanish Supervisory Authority regarding the Processor Binding Corporate Rules of Kumon Group
  - Opinion 07/2021 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of Kumon Group
  - Opinion 08/2021 on the draft decision of the Baden-Wurttemberg Supervisory Authority regarding the Processor Binding Corporate Rules of Luxoft Group
  - Opinion 09/2021 on the draft decision of the Baden-Wurttemberg Supervisory Authority regarding the Controller Binding Corporate Rules of Luxoft Group
  - Opinion 10/2021 on the draft decision of the competent Supervisory Authority of Hungary regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR
  - Opinion 11/2021 on the draft decision of the competent Supervisory Authority of Norway regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR
  - Opinion 12/2021 on the draft decision of the competent Supervisory Authority of Portugal regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR
  - Opinion 13/2021 on the draft decision of the competent Supervisory Authority of Romania regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR
  - Opinion 16/2021 on the draft decision of the Belgian Supervisory Authority regarding the “EU Data Protection Code of Conduct for Cloud Service Providers” submitted by Scope Europe
  - Opinion 17/2021 on the draft decision of the French Supervisory Authority regarding the European code of conduct submitted by the Cloud Infrastructure Service Providers (CISPE)
  - Opinion 18/2021 on the draft Standard Contractual Clauses submitted by the Lithuanian Supervisory Authority (Art. 28(8) GDPR)
  - Opinion 19/2021 on the draft decision of the competent

Supervisory Authority of Hungary regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR

- Opinion 21/2021 on the draft decision of the French Supervisory Authority regarding the Controller Binding Corporate Rules of the CGI Group
- Opinion 22/2021 on the draft decision of the French Supervisory Authority regarding the Processor Binding Corporate Rules of the CGI Group
- Opinion 23/2021 on the draft decision of the competent Supervisory Authority of Czech Republic regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR
- Opinion 24/2021 on the draft decision of the competent Supervisory Authority of Slovakia regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR
- Opinion 25/2021 on the draft decision of the competent Supervisory Authority of Lithuania regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR
- Opinion 26/2021 on the draft decision of the Supervisory Authority of North Rhine-Westphalia (Germany) regarding the Controller Binding Corporate Rules of the Internet Initiative Japan Group
- Opinion 27/2021 on the draft decision of the Supervisory Authority of North Rhine-Westphalia (Germany) regarding the Processor Binding Corporate Rules of the Internet Initiative Japan Group
- Opinion 28/2021 on the draft decision of the Belgian Supervisory Authority regarding the Controller Binding Corporate Rules of Oregon Tool, Inc (formerly “Blount”)
- Opinion 29/2021 on the draft decision of the Belgian Supervisory Authority regarding the Processor Binding

Corporate Rules of Oregon Tool, Inc (Formerly “Blount”)

- Opinion 30/2021 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of the COLT Group
- Opinion 31/2021 on the draft decision of the Spanish Supervisory Authority regarding the Processor Binding Corporate Rules of the COLT Group
- Opinion 33/2021 on the draft decision of the Belgian Supervisory Authority regarding the Controller Binding Corporate Rules of Carrier
- Opinion 34/2021 on the draft decision of the Belgian Supervisory Authority regarding the Controller Binding Corporate Rules of Otis
- Opinion 35/2021 on the draft decision of the competent Supervisory Authority of Belgium regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR
- Opinion 36/2021 on the draft decision of the competent Supervisory Authority of Norway regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR
- Opinion 37/2021 on the draft decision of the competent Supervisory Authority of Malta regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR
- Opinion 38/2021 on the draft decision of the competent Supervisory Authority of Latvia regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43(3) GDPR
- Opinion 39/2021 on whether Art. 58(2)(g) GDPR could serve as a legal basis for a supervisory authority to order ex officio the erasure of personal data, in a situation where such request was not submitted by the data subject

- Urgent Binding Decision 01/2021 on the request under Art. 66(2) GDPR from the Hamburg (German) Supervisory Authority for ordering the adoption of final measures regarding Facebook Ireland Limited
- Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Art. 65(1)(a) GDPR

## 8.3. JOINT OPINIONS ADOPTED IN 2021

- EDPB-EDPS Joint Opinion 01/2021 on standard contractual clauses between controllers and processors
- EDPB-EDPS Joint Opinion 02/2021 on standard contractual clauses for the transfer of personal data to third countries
- EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act)
- EDPB-EDPS Joint Opinion 04/2021 on the Proposal for a Regulation of the European Parliament and of the Council on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery
- EDPB-EDPS Joint Opinion 05/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)

## 8.4. LEGISLATIVE CONSULTATION

- Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom
- Opinion 15/2021 regarding the European Commission

Draft Implementing Decision pursuant to Directive (EU) 2016/680 on the adequate protection of personal data in the United Kingdom

- Opinion 20/2021 on Tobacco Traceability System
- Opinion 32/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the Republic of Korea
- EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research – 02/02/2021
- EDPB contribution to the 6th round of consultations on the draft Second Additional Protocol to the Council of Europe Budapest Convention on Cybercrime – 04/05/2021
- Statement 05/2021 on the Data Governance Act in light of the legislative developments – 19/05/2021
- Statement on the Digital Services Package and Data Strategy – 18/11/2021
- Contribution of the EDPB to the European Commission's evaluation of the Data Protection Law Enforcement Directive (LED) under Article 62 – 14/12/2021

## 8.5. OTHER DOCUMENTS

- Information note on data transfers under the GDPR to the United Kingdom after the transition period - update 13/01/2021
- Statement on the end of the Brexit transition period - update 13/01/2021
- Pre-GDPR BCRs overview list – 26/01/2021
- EDPB Work Programme 2021/2022 – 16/03/2021

## 8.6. LIST OF EXPERT SUBGROUPS WITH SCOPE OF MANDATES

NAME OF EXPERT SUBGROUP (ESG)	SCOPE OF MANDATE
<b>Borders, Travel &amp; Law Enforcement (BTLE) Expert Subgroup</b>	<ul style="list-style-type: none"> <li>• Law Enforcement Directive</li> <li>• Cross-border requests for e-evidence</li> <li>• Adequacy decisions under the Law Enforcement Directive, access to transferred data by law enforcement and national intelligence authorities in third countries</li> <li>• Passenger Name Records (PNR)</li> <li>• Border controls</li> </ul>
<b>Compliance, e-Government and Health (CEH) Expert Subgroup</b>	<ul style="list-style-type: none"> <li>• Codes of conduct, certification and accreditation</li> <li>• Compliance with public law and eGovernment</li> <li>• Processing of personal data concerning health</li> <li>• Processing of personal data for scientific research purposes</li> <li>• Consultation on several legislative proposals by the European Commission within the Digital Strategy</li> <li>• Close cooperation on DPIA with the Technology ESG focusing on the perspective of their mandates</li> <li>• Close cooperation on privacy by design and by default with the Technology ESG focusing on the perspective of their mandates</li> </ul>
<b>Cooperation Expert Subgroup</b>	<ul style="list-style-type: none"> <li>• General focus on procedures established by the GDPR for the purposes of the cooperation mechanism</li> <li>• Guidance on procedural questions linked to the cooperation mechanism</li> <li>• International mutual assistance and other cooperation tools to enforce the GDPR outside the EU (Art. 50 GDPR)</li> </ul>
<b>Coordinators Expert Subgroup</b>	<ul style="list-style-type: none"> <li>• General coordination between the Expert Subgroup Coordinators</li> <li>• Coordination on the annual Expert Subgroup working plan</li> </ul>

<b>Enforcement Expert Subgroup</b>	<ul style="list-style-type: none"> <li>• Mapping/analysing the need for additional clarifications or guidance, based on practical experiences with the application of Chapters VI, VII and VIII GDPR</li> <li>• Mapping/analysing possible updates of existing Cooperation subgroup tools</li> <li>• Monitoring of investigation activities</li> <li>• Practical questions on investigations</li> <li>• Guidance on the practical application of Chapter VII GDPR including exchanges on concrete cases</li> <li>• Guidance on the application of Chapter VIII GDPR together with the Taskforce on Administrative Fines</li> <li>• Art. 65 and Art. 66 procedures</li> </ul>
<b>Financial Matters Expert Subgroup</b>	<p>Application of data protection principles in the financial sector (e.g. automatic exchange of personal data for tax purposes; impact of FATCA on the protection of personal data; interplay between Second Payment Services Directive and GDPR)</p>
<b>International Transfers Expert Subgroup</b>	<p>Guidance on Chapter V (International transfer tools and policy issues), more specifically:</p> <ul style="list-style-type: none"> <li>• Review European Commission Adequacy decisions</li> <li>• Guidelines on Art. 46 GDPR and review of administrative arrangements between public authorities and bodies</li> <li>• Codes of conduct and certification as transfer tools</li> <li>• Art. 48 GDPR together with BTLE ESG</li> <li>• Art. 50 GDPR together with Cooperation ESG</li> <li>• Guidelines on territorial scope and the interplay with Chapter V of the GDPR – interaction with Key Provisions ESG</li> <li>• Exchange of information on review of BCRs and ad hoc contractual clauses according to Art. 64 GDPR</li> </ul>
<b>IT Users Expert Subgroup</b>	<p>Developing and testing IT tools used by the EDPB with a practical focus:</p> <ul style="list-style-type: none"> <li>• Collecting feedback on the IT system from users</li> <li>• Adapting the systems and manuals</li> <li>• Discussing other business needs including tele- and videoconference systems</li> </ul>

<b>Key Provisions Expert Subgroup</b>	Guidance on core concepts and principles of the GDPR, including Chapters I (e.g. scope, definitions like LSA and large-scale processing) and II (main principles); Chapters III (e.g. rights of individuals, transparency), IV (e.g. DPO – shared competences with CEH ESG, Enforcement ESG and Technology ESG) and IX
<b>Social Media Expert Subgroup</b>	<ul style="list-style-type: none"> <li>• Analysing social media services, conceived as online platforms that focus on enabling the development of networks and communities of users, among which information and content is shared and whereby additional functions provided by social media services include targeting, personalisation, application integration, social plug-ins, user authentication, analytics and publishing</li> <li>• Analysing established and emerging functions offered by social media, including the underlying processing activities and corresponding risks for the rights and freedoms of individuals</li> <li>• Developing guidance, recommendations and best practices in relation to both the offer and use of social media functions, in particular for economic or political reasons</li> <li>• Providing assistance to other subgroups, in particular by proposing strategic priorities in terms of (a) supervision and (b) the development of new EDPB guidance or updating of existing WP29 guidance</li> </ul>
<b>Strategic Advisory Expert Subgroup</b>	<ul style="list-style-type: none"> <li>• Guidance on strategic questions affecting the whole EDPB (including the discussion on the strategy and on the work plans of the ESGs)</li> <li>• Clarification of questions that could not be resolved in the ESG</li> </ul>
<b>Taskforce on Administrative Fines</b>	Development of Guidelines on the harmonisation of the calculation of fines
<b>Technology Expert Subgroup</b>	<ul style="list-style-type: none"> <li>• Technology, innovation, information security, confidentiality of communication in general</li> <li>• ePrivacy, encryption</li> <li>• DPIA and data breach notifications</li> <li>• Emerging technologies, innovation and other challenges related to privacy: reflecting on data protection risks of future technological developments</li> <li>• Providing input on technology matters relevant to other ESG</li> </ul>

## **CONTACT DETAILS**

Postal address  
Rue Wiertz 60, B-1047 Brussels

Office address  
Rue Montoyer 30, B-1000 Brussels

**CORRIGENDUM  
to the EDPB Annual Report 2022**

On page 70, last paragraph,

for:

*“Pursuant to Art. 62 of Regulation 2018/1725, the following EU large-scale IT systems, bodies, offices and agencies currently fall under the CSC’s scope:”*,

read:

*“Pursuant to Art. 62 of Regulation 2018/1725 or with the EU legal act establishing the large scale IT system or the EU body, office or agency, the following EU large-scale IT systems, bodies, offices and agencies currently fall under the CSC’s scope:”*.

On page 71, second paragraph,

for:

*“• Eurojust, the agency responsible for judicial cooperation in criminal matters among EU Member States;*

- European Public Prosecutor Office (EPPO), the prosecution agency responsible for investigating, prosecuting and bringing to judgment crimes against the EU budget;*
- European Union Agency for Law Enforcement Cooperation (Europol).”*

read:

*“• Eurojust, the agency responsible for judicial cooperation in criminal matters among EU Member States*

- European Union Agency for Law Enforcement Cooperation (Europol).*

*The CSC also provides a forum for cooperation in the context of the European Public Prosecutor Office (EPPO), the prosecution body responsible for investigating, prosecuting and bringing to judgment crimes against the EU budget.”.*

# ANNUAL REPORT 2022

## STREAMLINING ENFORCEMENT THROUGH COOPERATION



edpb



European Data Protection Board



# TABLE OF CONTENTS

<b>1</b>	<b>GLOSSARY</b>	<b>4</b>	<b>3.2.3.</b>	Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR) and Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65 GDPR)	<b>13</b>
<b>2</b>	<b>FOREWORD</b>	<b>7</b>	<b>3.2.4.</b>	Binding Decision 5/2022 on the dispute submitted by the Irish SA regarding WhatsApp Ireland Limited (Art. 65 GDPR)	<b>14</b>
<b>3</b>	<b>2022 – HIGHLIGHTS</b>	<b>9</b>			
<b>3.1.</b>	<b>ENFORCEMENT COOPERATION</b>	<b>9</b>	<b>4</b>	<b>2022 - THE EDPB SECRETARIAT</b>	<b>16</b>
<b>3.1.1.</b>	Vienna statement on enforcement cooperation	10	<b>4.1.</b>	<b>THE EDPB SECRETARIAT</b>	<b>16</b>
<b>3.1.2.</b>	Guidelines 02/2022 on the application of Art. 60 GDPR	10	<b>4.2.</b>	<b>EDPB BUDGET</b>	<b>17</b>
<b>3.1.3.</b>	Guidelines 04/2022 on the calculation of administrative fines under the GDPR	11	<b>4.3.</b>	<b>IT COMMUNICATION TOOLS</b>	<b>17</b>
<b>3.2.</b>	<b>2022 ARTICLE 65 DECISIONS</b>	<b>12</b>	<b>4.4.</b>	<b>THE EDPB SECRETARIAT'S ACTIVITIES RELATING TO ACCESS TO DOCUMENTS</b>	<b>17</b>
<b>3.2.1.</b>	Decision 01/2022 on the dispute arisen on the draft decision of the French Supervisory Authority regarding Accor SA under Art. 65(1)(a) GDPR	12	<b>4.5.</b>	<b>THE EDPB SECRETARIAT'S DATA PROTECTION OFFICER ACTIVITIES</b>	<b>18</b>
<b>3.2.2.</b>	Binding Decision 2/2022 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Meta Platforms Ireland Limited (Instagram) under Art. 65(1)(a) GDPR	12			
<b>5</b>	<b>ACTIVITIES IN 2022</b>	<b>20</b>			
<b>5.1.</b>	<b>BINDING DECISIONS</b>	<b>20</b>			

# EDPB Annual Report 2022

<b>5.1.1.</b>	Decision 01/2022 on the draft decision of the French Supervisory Authority regarding Accor SA under Art. 65(1)(a) GDPR	20	<b>5.3. GENERAL GUIDANCE</b>	<b>25</b>
<b>5.1.2.</b>	Binding Decision 2/2022 on the draft decision of the Irish Supervisory Authority regarding Meta Platforms Ireland Limited (Instagram) under Art. 65(1)(a) GDPR	21	<b>5.3.1.</b> Guidelines 01/2022 on data subject rights - Right of access	25
<b>5.1.3.</b>	Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR) and Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65 GDPR)	21	<b>5.3.2.</b> Guidelines 02/2022 on the application of Art. 60 GDPR	26
<b>5.1.4.</b>	Binding Decision 5/2022 on the dispute submitted by the Irish SA regarding WhatsApp Ireland Limited (Art. 65 GDPR)	22	<b>5.3.3.</b> Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them	26
<b>5.2. CONSISTENCY OPINIONS</b>	<b>22</b>	<b>5.3.4.</b> Guidelines 04/2022 on the calculation of administrative fines under the GDPR	26	
<b>5.2.1.</b>	Opinions on draft decisions regarding Binding Corporate Rules	22	<b>5.3.5.</b> Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement	27
<b>5.2.2.</b>	Opinions on draft requirements for accreditation of a certification body	24	<b>5.3.6.</b> Guidelines 06/2022 on the practical implementation of amicable settlements	27
<b>5.2.3.</b>	Opinions on certification criteria	24	<b>5.3.7.</b> Guidelines 07/2022 on certification as tool for transfers	27
<b>5.2.4.</b>	Opinions on SAs' approval of accreditation requirements for code of conduct monitoring body	25	<b>5.3.8.</b> Guidelines 8/2022 on identifying a controller or processor's LSA	28
		<b>5.3.9.</b> Guidelines 9/2022 on personal data breach notification under GDPR	28	
		<b>5.3.10.</b> Guidelines adopted after public consultation	28	
		<b>5.4. REGISTER FOR DECISIONS TAKEN BY SA AND COURTS ON ISSUES HANDLED IN THE CONSISTENCY MECHANISM</b>	<b>29</b>	

<b>5.5. LEGISLATIVE CONSULTATION AND DOCUMENTS ADDRESSED TO THE EU INSTITUTIONS OR NATIONAL AUTHORITIES</b>	<b>30</b>	<b>5.6. OTHER GUIDANCE AND INFORMATION NOTES</b>	<b>34</b>
5.5.1. EDPB-EDPS Joint Opinion 1/2022 on the extension of the Covid-19 certificate Regulation	30	5.6.1. Statement 02/2022 on personal data transfers to the Russian Federation	34
5.5.2. EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)	30	<b>5.7. GDPR COOPERATION AND ENFORCEMENT</b>	<b>35</b>
5.5.3. EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space	31	5.7.1. Statement on enforcement cooperation	35
5.5.4. EDPB-EDPS Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse	32	5.7.2. EDPB Document on the selection of cases of strategic importance	35
5.5.5. Statement 01/2022 on the announcement of an agreement in principle on a new Trans-Atlantic Data Privacy Framework	33	5.7.3. Coordinated Enforcement Framework	36
5.5.6. Statement 04/2022 on the design choices for a digital euro from the privacy and data protection perspective	33	5.7.4. Support Pool of Experts	36
5.5.7. Response of the EDPB to the European Commission's targeted consultation on a digital Euro	33	<b>5.8. PLENARY MEETINGS AND SUBGROUPS</b>	<b>36</b>
5.5.8. Statement on the implications of the CJEU judgement C-817/19 on the use of PNR in Member States	34	<b>5.9. STAKEHOLDER CONSULTATION</b>	<b>37</b>
		5.9.1. Stakeholder events	37
		5.9.2. Public consultation on draft guidance	37
		5.9.3. Survey on practical application of adopted guidance	38
		<b>5.10. EXTERNAL REPRESENTATION OF THE BOARD</b>	<b>39</b>
		<b>6. SUPERVISORY AUTHORITY ACTIVITIES IN 2022</b>	<b>40</b>
		<b>6.1. CROSS-BORDER COOPERATION</b>	<b>40</b>
		6.1.1. Preliminary procedure to identify the Lead and Concerned Supervisory Authorities	40
		6.1.2. Database regarding cases with a cross-border component	41

<b>6.1.3.</b>	One-Stop-Shop Mechanism and decisions	41
<b>6.1.4.</b>	Mutual Assistance	51
<b>6.1.5.</b>	Joint Operations	51
<b>6.2.</b>	<b>NATIONAL CASES</b>	<b>51</b>
<b>6.2.1.</b>	Some relevant national cases with exercise of corrective powers	51
<b>6.3.</b>	<b>SA SURVEY - BUDGET AND STAFF</b>	<b>69</b>

<b>7</b>	<b>COORDINATED SUPERVISION COMMITTEE OF THE LARGE EU INFORMATION SYSTEMS AND OF EU BODIES, OFFICES AND AGENCIES</b>	<b>70</b>
----------	---	-----------

<b>8</b>	<b>ANNEXES</b>	<b>72</b>
<b>8.1.</b>	<b>GENERAL GUIDANCE ADOPTED IN 2022</b>	<b>72</b>
<b>8.2.</b>	<b>CONSISTENCY OPINIONS AND DECISIONS ADOPTED IN 2022</b>	<b>72</b>
<b>8.3.</b>	<b>JOINT OPINIONS ADOPTED IN 2022</b>	<b>74</b>
<b>8.4.</b>	<b>LEGISLATIVE CONSULTATION</b>	<b>74</b>
<b>8.5.</b>	<b>OTHER DOCUMENTS</b>	<b>75</b>
<b>8.6.</b>	<b>LIST OF EXPERT SUBGROUPS AND TASKFORCES WITH SCOPE OF MANDATES</b>	<b>76</b>

# 1

## GLOSSARY

<b>Adequacy decision</b>	An implementing act adopted by the European Commission, stating that a non-EU country ensures an adequate level of protection of personal data.
<b>Binding Corporate Rules (BCRs)</b>	Data protection policies adhered to by controllers or processors established in the EU for transfers of personal data to controllers or processors outside the EU within a group of undertakings or enterprises or groups of enterprises engaged in a joint economic activity.
<b>Charter of Fundamental Rights of the EU</b>	A legally binding Charter that sets out the civil, political, economic, social and cultural rights of EU citizens and residents (including the right to the protection of personal data in its Art. 8).
<b>Concerned Supervisory Authorities (CSAs)</b>	A Supervisory Authority concerned by the processing of personal data because: (a) the controller or processor is established on the territory of its Member State; (b) data subjects residing in the Member State are substantially affected by the processing; or (c) a complaint has been lodged with that Supervisory Authority.
<b>Court of Justice of the European Union (CJEU)</b>	The highest court in the EU judiciary system, which ensures uniform interpretation and application of EU law in EU Member States. It ensures those States and EU institutions abide by EU law.
<b>Cross-border processing</b>	Either (a) processing of personal data that takes place in the context of the activities of establishments in more than one Member State due to the controller or processor being established in more than one Member State; or (b) processing of personal data that takes place in the context of the activities of a controller or processor established in a single Member State, but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

<b>Data controller</b>	The natural or legal person, public authority, agency or other body that, 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 EU or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
<b>Data minimisation</b>	A principle that means that personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
<b>Data processor</b>	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
<b>Data Protection Impact Assessment (DPIA)</b>	An impact assessment aiming to evaluate the processing of personal data, including notably a description of the processing and its purposes, an assessment of the necessity and proportionality, an assessment of the risks for the rights and freedom of individuals, and the measures envisaged to address the risks.
<b>Data Protection Officer (DPO)</b>	An expert on data protection, who operates independently within an organisation to ensure the internal application of data protection.
<b>Data subject</b>	The person whose personal data is processed.
<b>European Commission</b>	An EU institution that shapes the EU's overall strategy, proposes new EU laws and policies, monitors their implementation and manages the EU budget.
<b>European Economic Area (EEA) Member States</b>	EU Member States and Iceland, Liechtenstein and Norway.
<b>European Union (EU)</b>	An economic and political union between 27 European countries.
<b>General Data Protection Regulation (GDPR)</b>	An EU Regulation that sets out rules on the rights of data subjects, the duties of data controllers and processors processing personal data, international data transfers and the powers of Supervisory Authorities.
<b>Lead Supervisory Authority (LSA)</b>	The Supervisory Authority where the “main establishment” of a data controller or processor is based, which has the primary responsibility for dealing with a cross-border data processing activity and for coordinating any cross-border investigation.

<b>Main establishment</b>	Either (a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union; unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment; or (b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union; or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under the GDPR.
<b>One-Stop-Shop mechanism</b>	A mechanism whereby the Supervisory Authority with the “main establishment” of a controller or processor in the EU serves as the Lead Supervisory Authority to ensure cooperation between Supervisory Authorities in the case of cross-border processing.
<b>Personal data</b>	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.
<b>Processing</b>	Any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
<b>Standard Contractual Clauses (SCCs)</b>	A set of contractual clauses that provide adequate safeguards for data transfers from the EU or the EEA to third countries and govern the relationship between involved controllers and processors.
<b>Supervisory Authority (SA) or Data Protection Authority (DPA)</b>	An independent public supervisory body that monitors the application of the GDPR and other national laws relating to data protection, in order to protect the rights and freedoms of natural persons in relation to the processing of personal data.
<b>Third country</b>	A country outside the EU and EEA.

# 2

## FOREWORD



It is my pleasure to introduce the fifth Annual Report of the European Data Protection Board (EDPB), also the last one published during my mandate as EDPB Chair.

Once again, this Report clearly demonstrates how much work is done by the EDPB in the span of a year, in terms of issuing guidance, consistency documents, legal advice and adopting binding decisions. What is also abundantly clear from this report is how the role of the EDPB has changed.

Today, we are much further than we were in 2018. The GDPR is at the heart of the newly adopted digital single market legislation, which will determine how large online platforms operate in the decades to come. Enforcement of data protection is now making headlines every week. Organisations worldwide are aware they cannot do business in Europe without complying with the GDPR.

Today, the EDPB is a major player in the European Economic Area (EEA) digital economy. It does not just ensure that data protection law is applied consistently across the EEA, but it helps shape Europe's digital future.

On top of being a source of guidance and legal advice, the EDPB has taken a series of important binding decisions in concrete cases in the past year. These decisions have a

far-reaching impact and the potential to change the way large digital players handle our personal data, today and in the future. We thereby help redress a balance that has been tipped too far in favour of large tech companies.

While enforcement has accelerated, there is still a lot we can and are planning to do to make sure the GDPR has the largest impact possible on the protection of people's data protection rights.

In April 2022, EDPB members gathered in my hometown Vienna with a view to finding solutions for more efficient enforcement cooperation. This meeting signalled a commitment of all Data Protection Authorities' (DPA) to deepen cooperation. Numerous initiatives to increase the DPAs' capacity to enforce were agreed upon. We also adopted a list of national administrative procedures that we would like to see streamlined. It is very positive that the European Commission has agreed to take a legislative initiative for greater harmonisation of these procedures, as this will help unlock the GDPR's potential.

It is also important to underline that the depth and breadth of our work could not have materialised without the efforts of everyone involved at the EDPB, and, not in the least, at the EDPB Secretariat. The EDPB Secretariat is a small and very dedicated group of people, without whose efforts and expertise the EDPB would not be able to achieve everything it sets out to do. It is important that we continue to supply the Secretariat with sufficient resources, so that they can provide much needed logistical, administrative and analytical and legal support to the EDPB.

The first five years of the EDPB's existence were the beginning of a process, whereby this new EU body gradually expanded its impact. The next five years will almost certainly bring new challenges, with even more enforcement and, as a result, more litigation too. I am confident that the EDPB will successfully face these new challenges, under the leadership of my successor.

**Andrea Jelinek**

**Chair of the European Data Protection Board**

# 3

## 2022 – HIGHLIGHTS

### 3.1. ENFORCEMENT COOPERATION

The EDPB plays a key role in enforcing data protection laws. It ensures consistent enforcement and promotes enforcement cooperation amongst SAs. In addition, for a small number of complex cases on which SAs cannot agree via consensus, the EDPB takes binding decisions.

*"Consistent enforcement is at the heart of the EDPB's work."*

- Dr Andrea Jelinek, Chair of the EDPB

Since the General Data Protection Regulation (GDPR) started applying, the EDPB has focused attention and effort on ensuring consistent enforcement based on cooperation. Following the vision laid down in its [2021-2023 Strategy](#), this continues to be a high priority for the EDPB. In that respect, in 2022, the EDPB's work

on enforcement cooperation shifted into a higher gear, particularly through the numerous initiatives taken to streamline enforcement cooperation among SAs.

It is worth highlighting the following initiatives:

- A number of taskforces have worked on key topics with a cross-border dimension. This has led to a consistent approach by the SAs on topics such as Google Analytics and cookie banners.
- Following the creation of the Coordinated Enforcement Framework in 2021 for simultaneous and coordinated enforcement actions by SAs, in 2022, 22 SAs undertook coordinated investigations into over 90 cloud services used in the public sector throughout the EEA.
- To support and increase SAs' capacity to supervise, investigate and enforce, the EDPB launched a [Support Pool of Experts](#) with

specialists in various areas, including IT auditing, security and data science.

All these efforts contribute to better internal work processes, unified strategies, enhanced cooperation and overall streamlining of the enforcement.

### **3.1.1. VIENNA STATEMENT ON ENFORCEMENT COOPERATION**

In pursuit of developing a comprehensive and collaborative approach to address issues related to GDPR enforcement, the EDPB Members met in Vienna in April 2022 and reiterated their commitment to close cross-border cooperation. A statement summarised the Members' agreed action towards strong and swift enforcement of the GDPR through further enhancing cooperation on strategic cases and diversifying the range of cooperation methods used. Among other topics, the EDPB agreed to identify a list of procedural aspects that could be further harmonised in EU law to maximise the positive impact of GDPR cooperation. This list was sent to the European Commission for its consideration in October 2022, and was added to the European Commission's work programme for 2023.

Going forward, the EDPB will also prioritise enforcement actions by fostering greater cooperation on cross-border cases of strategic importance, addressing legal challenges stemming from matters of general application, and better aligning national enforcement strategies.

The EDPB Members are cognisant of the fact that this will represent a collaborative approach, with dedicated effort and cooperation from every member in improving the GDPR enforcement. As a consequence, this will result in greater robustness of the enforcement process and in ensuring a consistent interpretation of the GDPR.

Adopted: 28 April 2022

### **3.1.2. GUIDELINES 02/2022 ON THE APPLICATION OF ART. 60 GDPR**

In line with the broader narrative to support effective enforcement and efficient cooperation between national SAs, the EDPB adopted Guidelines 02/2022 focusing on the interactions of SAs with each other, the EDPB and third parties under Art. 60 GDPR. The aim is to provide guidance in terms of cooperation and the One-Stop-Shop (OSS) mechanism. In practice, this helps SAs to enact their own national procedures in a manner consistent with the cooperation under the OSS mechanism.

The guidelines elaborate and clarify the requirements of each paragraph of Art. 60 GDPR, based on the provision's text and its practical implementation.

In terms of Art. 60(1) GDPR, the guidelines emphasise that the principles to be followed throughout the whole cooperation procedure are mutual obligations and that the SAs should endeavour to reach a consensual decision that is embedded in a process of mutual, consistent and timely exchange of all relevant information.

The guidance on Art. 60(2) GDPR focuses on the cooperative aspects in cases where the Lead Supervisory Authority (LSA) asks Concerned Supervisory Authorities (CSAs) to provide mutual assistance (Art. 61 GDPR) and conduct joint operations (Art. 62 GDPR).

The part dedicated to Art. 60(3) GDPR highlights the importance of collaborative interaction and early exchange of information between the LSA and the CSAs. More specifically, the guidelines clarify that the CSA should be able to contribute to the overall cooperation procedure and express their views even before the creation of a draft decision. In addition, the LSA is under the obligation to submit a draft decision in all cases of cross-border processing. The guidance on Art. 60(4)-(6) GDPR covers the potential scenarios that

follow the submission of a draft decision by the LSA and adds consistency to the post-submission procedure. The guidance on Art. 60(7)-(9) GDPR clarifies the distinction between notifying and informing SAs following the adoption of a binding decision.

To ensure further compliance after a final decision has been made by the LSA, the EDPB provides guidance on Art. 60(10) GDPR in terms of the obligations of the controller or processor in further processing activities in all its establishments.

Overall, the provided clarification and guidance of the requirements under Art. 60 GDPR significantly contribute to the desired consistency of the SAs' work and in enhancing enforcement cooperation.

Adopted: 14 March 2022

### **3.1.3. GUIDELINES 04/2022 ON THE CALCULATION OF ADMINISTRATIVE FINES UNDER THE GDPR**

To harmonise the approach used by SAs in calculating fines, the EDPB adopted the first version of Guidelines 04/2022. The guidelines contribute to an important part of the EDPB's strategy in creating more efficient cooperation among SAs on cross-border cases.

*"From now on, SAs across the EEA will follow the same methodology to calculate fines. This will boost further harmonisation and transparency of the fining practice of SAs. The individual circumstances of a case must always be a determining factor and SAs have an important role in ensuring that each fine is effective, proportionate and dissuasive."*

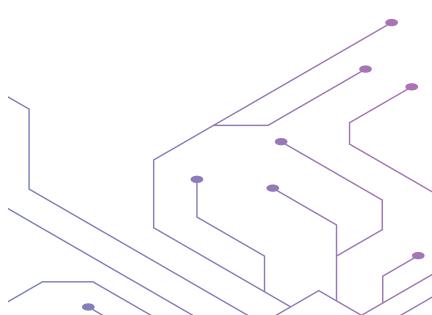
- Dr Andrea Jelinek, Chair of the EDPB

The EDPB devised a systematic and chronological five-step methodology that SAs across the European Economic Area (EEA) can use for calculating administrative fines for infringements of the GDPR.

- 1.** The SAs have to assess whether the case at stake concerns one or more sanctionable conducts and whether this has led to one or multiple infringements. Furthermore, in case one conduct gives rise to multiple infringements, it needs to be determined whether one infringement precludes the attribution of another infringement, or whether they are to be attributed alongside each other. The aim is to clarify which infringements can result in fines.
- 2.** The SAs should use a harmonised starting point for the calculation of a fine, with three elements to consider: the categorisation of infringements by nature, the seriousness of the infringement and the turnover of the undertaking. This starting point forms the foundation for further calculations, and each assessment needs to be based on the merits of the case.
- 3.** The SAs should also determine whether there are aggravating and mitigating circumstances (as listed in Art. 83 (2) GDPR) and increase or decrease the fine accordingly.
- 4.** The SAs must ensure that fines do not exceed the legal maximums as set out in Art. 83(4)-(6) GDPR.
- 5.** The SAs need to assess whether the calculated final amount meets the requirements of effectiveness, dissuasiveness and proportionality, or whether further adjustments to the amount are necessary.

The EDPB will regularly revise the guidelines and proposed methodology.

Adopted: 12 May 2022



## 3.2. 2022 ARTICLE 65 DECISIONS

The EDPB is empowered to issue binding decisions under Art. 65 GDPR to guarantee the consistent application of the GDPR by SAs. In 2022, the EDPB issued 5 binding decisions addressing a range of issues from right to access, right to object direct marketing, protection of children's use of social media to legal basis for processing personal data.

### **3.2.1. DECISION 01/2022 ON THE DISPUTE ARISEN ON THE DRAFT DECISION OF THE FRENCH SUPERVISORY AUTHORITY REGARDING ACCOR SA UNDER ART. 65(1)(A) GDPR**

In June 2022, the EDPB settled a dispute regarding a fine against the French hospitality company Accor SA in its Decision 01/2022.

The French LSA issued a draft decision against Accor SA following complaints relating to a failure to consider the right to object to the receipt of marketing messages by mail and/or difficulties encountered in exercising the right of access. Upon sharing the draft decision with the CSAs, the Polish SA raised three objections, with a primary focus on the amount of the fine, which in its opinion was not effective, proportionate and dissuasive enough. The SAs did not reach a consensus on that given issue, henceforth it was referred to the EDPB pursuant to Art. 65(1)(a) GDPR.

The EDPB agreed with the reasoning of the Polish SA in certain aspects and decided that the French LSA needed to reassess the elements it relied upon to calculate the amount of the fine in order to ensure that it meets the criterion of dissuasiveness. The EDPB clarified that the fine should be determined solely based on the company's turnover of the preceding year, namely 2021, without considering the reduced turnover caused by the COVID-19 pandemic as a mitigating factor under 83(2)(k) GDPR.

The GDPR fine issued to Accor was increased from the initial EUR 100,000 imposed by the French LSA to EUR 500,000 following the EDPB's binding decision.

Adopted: 15 June 2022

### **3.2.2. BINDING DECISION 2/2022 ON THE DISPUTE ARISEN ON THE DRAFT DECISION OF THE IRISH SUPERVISORY AUTHORITY REGARDING META PLATFORMS IRELAND LIMITED (INSTAGRAM) UNDER ART. 65(1)(A) GDPR**

In July 2022, the EDPB adopted a binding decision regarding Instagram, a unit of Meta Platforms Ireland Limited (Meta IE), particularly on the policy of maintaining public-by-default profiles of children and the mandatory public disclosure of their contact details when operating business accounts.

The Irish LSA triggered the dispute resolution procedure under Art. 65 GDPR after no compromise had been reached on the objections raised by several CSAs concerning the legal basis for processing and the determination of the fine.

In terms of publicly disclosing children's contact details when they operate business accounts, Meta IE relied on two legal bases for processing personal data: "performance of a contract" and "legitimate interests". The EDPB found that Meta IE could not have relied on Art. 6(1)(b) GDPR (performance of a contract) as a legal basis for the publication since the processing at stake was not necessary for the performance of a contract between Meta IE and its child users. Regarding the alternative legal basis of Art. 6(1)(f) GDPR (legitimate interests), the EDPB concluded that the publication of the children's contact details did not meet the requirements because the processing was either unnecessary or, if it were to be considered necessary, it did not pass the balancing test required when determining legitimate interests.

Therefore, the EDPB concluded that Meta IE unlawfully processed children's personal data and it further instructed the Irish LSA to amend its draft decision by including the infringement of Art. 6(1) GDPR.

The EDPB also instructed the Irish SA to assess its envisaged administrative fine in accordance with Art. 83(1)-(2) GDPR to:

- Impose an effective, proportionate and dissuasive administrative fine for the additional infringement; and
- Ensure that the final amounts of the administrative fines are effective, proportionate and dissuasive.

On the issue of public-by-default profiles of children, initially raised as an objection by the Norwegian SA, the Irish SA was not required to amend its draft decision. Indeed, the EDPB concluded that the objection did not meet the requirements of being "relevant and reasoned" under Art. 4(24) GDPR since it was neither relevant nor sufficiently reasoned against the backdrop of the legal and factual content of the Irish SA's draft decision.

Following the EDPB's binding decision, the Irish LSA adopted its final decision against Meta IE. They determined that Meta IE had infringed Art. 6(1) GDPR. The final fine was the maximum of the EUR 202-405 million range which was initially envisaged in the draft decision.

*"This is a historic decision. Not just because of the height of the fine - this is the second highest fine since the entry into application of the GDPR - it is also the first EU-wide decision on children's data protection rights. With this binding decision, the EDPB makes it extra clear that companies targeting children have to be extra careful. Children merit*

*specific protection with regard to their personal data."*

- Dr Andrea Jelinek, Chair of the EDPB

This EDPB decision has practical repercussions on the way this online platform operates its services in the EU. Meanwhile, Instagram has changed its practices. Accounts of people under 18 years of age are now private-by-default in the UK and EU, and the disclosure of contact details for business accounts is no longer mandatory.

Adopted: 28 July 2022

### **3.2.3. BINDING DECISION 3/2022 ON THE DISPUTE SUBMITTED BY THE IRISH SA ON META PLATFORMS IRELAND LIMITED AND ITS FACEBOOK SERVICE (ART. 65 GDPR) AND BINDING DECISION 4/2022 ON THE DISPUTE SUBMITTED BY THE IRISH SA ON META PLATFORMS IRELAND LIMITED AND ITS INSTAGRAM SERVICE (ART. 65 GDPR)**

Following the EDPB's [binding dispute resolution decisions](#) of 5 December 2022, the Irish SA adopted its decisions regarding Facebook and Instagram (Meta IE). These decisions are the result of complaint-based inquiries into Facebook's and Instagram's activities in particular concerning the lawfulness and transparency of processing for behavioural advertising.

The binding decisions were adopted on the basis of Art. 65(1)(a) GDPR, after the Irish SA as LSA had triggered two dispute resolution procedures concerning the objections raised by concerned supervisory authorities (CSAs) from ten countries in each case. Among others, CSAs issued objections concerning the legal basis for processing (Art. 6 GDPR), data protection principles (Art. 5 GDPR), and the use of corrective measures including fines.

The EDPB decided that Meta IE inappropriately relied on contract as a legal basis to process personal data in the context of Facebook's Terms of Service and Instagram's Terms of Use for the purpose of behavioural advertising as this was not a core element of the services. The EDPB found in both cases that Meta IE lacked a legal basis for this processing and therefore unlawfully processed these data. As a consequence, the EDPB instructed the Irish SA to amend the finding in its draft decisions and to include an infringement of Art. 6(1) GDPR.

The EDPB instructed the Irish SA to include, in its final decisions, an order for Meta IE to bring its processing of personal data for behavioural advertising in the context of the Facebook and Instagram services into compliance with Art. 6(1) GDPR within three months.

Next, the EDPB examined whether the complaints had been addressed with due diligence. The complainant had raised the fact that sensitive data is processed by Meta IE. However, the Irish SA did not assess processing of sensitive data and therefore, the EDPB did not have sufficient factual evidence to enable it to make findings on any possible infringement of the controller's obligations under Art. 9 GDPR. As a result, the EDPB disagreed with the Irish SA's proposed conclusion that Meta IE is not legally obliged to rely on consent to carry out the processing activities involved in the delivery of its Facebook and Instagram services, as this could not be categorically concluded without further investigations. Therefore, the EDPB decided that the Irish SA must carry out a new investigation.

In addition, the EDPB instructed the Irish SA to include in both final decisions a finding of infringement of the principle of fairness and to adopt the appropriate corrective measures. The EDPB noted that the grave breaches of transparency obligations impacted the reasonable expectations of the users, that Meta IE had presented its services to users in a misleading manner, and that the relationship between Meta IE and users was imbalanced.

With respect to the administrative fines, the EDPB directed the Irish SA to impose an administrative fine for the additional infringements of Art. 6(1) GDPR (lack of legal basis for the processing of personal data) and to issue significantly higher fines for the transparency infringements identified, as it found the fines proposed did not fulfil the requirement of being effective, proportionate and dissuasive. This led to the Irish SA significantly increasing the fines in its final decisions (from a maximum of EUR 36 million and EUR 23 million for the Facebook and Instagram draft decisions, to EUR 210 million and EUR 180 million in the final decisions respectively).

### **3.2.4. BINDING DECISION 5/2022 ON THE DISPUTE SUBMITTED BY THE IRISH SA REGARDING WHATSAPP IRELAND LIMITED (ART. 65 GDPR)**

Following the EDPB's binding dispute resolution decision of December 5th, WhatsApp Ireland Limited (WhatsApp IE) was issued a EUR 5.5 million fine by the Irish SA.

In its Binding Decision, the EDPB instructed the Irish SA to amend its draft decision with respect to the findings concerning lawfulness of the processing and the principle of fairness, and to the corrective measures envisaged.

Regarding the lawfulness of processing for Service improvement purposes, the EDPB decided that WhatsApp IE inappropriately relied on contract as a legal basis to process personal data. As a consequence, the EDPB instructed the Irish SA to add an infringement of Art. 6(1) GDPR. Additionally, the EDPB instructed the Irish SA to include an infringement of the principle of fairness under Art. 5(1)(a) GDPR.

The EDPB further decided that the Irish SA must carry out an investigation into WhatsApp IE's processing operations in order to determine whether it processes special categories of personal data (Art. 9 GDPR);

whether it processes data for the purposes of behavioural advertising, for marketing purposes, as well as for the provision of metrics to third parties and the exchange of data with affiliated companies for the purposes of service improvements.

With respect to corrective measures, the EDPB requested the Irish SA to include in its final decision an order for WhatsApp IE to bring its processing of personal data for the purposes of service improvement in the context of its Terms of Service into compliance with Art. 6(1) GDPR within a specified period of time, and to cover the infringements of Art. 6(1) GDPR with an administrative fine.

# 4

## 2022 - THE EDPB SECRETARIAT

### 4.1. THE EDPB SECRETARIAT

The EDPB Secretariat, which is provided by the European Data Protection Supervisor (EDPS), offers analytical, administrative and logistical support to the EDPB. The EDPB Secretariat is in charge of drafting EDPB documents, providing IT solutions to ensure transparent communications between all the European national Supervisory Authorities (SAs), handling EDPB media relations, as well as organising all EDPB meetings.

A [Memorandum of Understanding](#) establishes the terms of this cooperation between the EDPB and the EDPS. The staff at the EDPB Secretariat are employed by the EDPS, however, they work exclusively under the instructions of the Chair of the EDPB. At the end of 2022, the staff of the EDPB Secretariat was composed of 30 FTE staff members: one head of the EDPB

Secretariat, 1 deputy head of unit, 1 head of sector, 4 heads of activity, 11 legal officers, 4 communication officers, 6 administrative assistants and 2 IT officers.

The EDPB Secretariat led the drafting of 26 opinions, binding decisions and statements adopted by the EDPB in 2022 and contributed to further 23 guidelines, opinions, binding decisions, statements and recommendations.

In 2022, the EPDB Secretariat organised 347 meetings for the EDPB, including 15 plenary meetings, 160 expert subgroup or taskforce meetings and 172 drafting teams. One significant distinction from previous years is that in 2022, the EDPB convened hybrid meetings for the first time. Out of 347 meetings, 34 were hybrid, whereas 308 were held remotely and 5 took place in-person.

## 4.2. EDPB BUDGET

The EDPB budget forms part of the broader budget of the EDPS. The financial resources provided to the data protection institutions allow them to fulfil their tasks, contribute to the implementation of the democratic values of the EU and the fundamental rights of privacy and data protection.

The EDPB budget for 2022 amounts to EUR 6,812,000 and covers all aspects related to the functioning of the EDPB. This includes, but is not limited to, expenditure for EDPB meetings at the plenary and subgroup level, translation and interpretation costs, IT services, and remuneration of the EDPB Secretariat staff.

## 4.3. IT COMMUNICATION TOOLS

In the context of cooperation between SAs, the EDPB Secretariat provides continuous support to SAs with IT solutions that facilitate their communication. In this respect, the EDPB Secretariat leads the IT Users Expert Subgroup, which focuses on the need for development and making changes to the information systems used by EDPB, including the Internal Market Information (IMI) system which is used to exchange information necessary for the GDPR cooperation and consistency mechanism. This included the overhaul of two procedures to reflect the experience gathered in the first years of the GDPR and updates to reflect modifications in the EDPB's Rules of Procedure. In addition, further reporting possibilities were introduced.

Throughout 2022, the EDPB Secretariat continued working on best practices to refine the procedures in use and to share its expertise on the use of the IMI system. While employing the IMI system, the SAs and the European Commission are supported by the EDPB IMI helpdesk within the EDPB Secretariat. The IMI helpdesk continued to carry out 3252 proactive monitoring procedures to ensure that case files were complete and registered correctly.

The EDPB Secretariat also performed a follow-up to the migration of the EDPB Wiki platform used for internal sharing of information, with additional functionalities and an enhanced user experience. In addition, the EDPB Secretariat upgraded the content management system (CMS) of the EDPB website '<https://edpb.europa.eu>', which manages the creation and modification of digital content, to Drupal 9. A new advanced search feature to improve the usability of the website was introduced. The EDPB website was visited 275,734 times in 2022 and the most clicked topics are international transfer of data, General Data Protection Regulation, Data Protection Impact Assessment (DPIA) and code of conduct. Considerable efforts were made regarding the translation of documents available on the website. In fact, 283 EDPB documents and 159 press releases were translated into 22 languages.

The EDPB Secretariat improved internal tools for the organisation and planning of meetings and for the management of documents.

## 4.4. THE EDPB SECRETARIAT'S ACTIVITIES RELATING TO ACCESS TO DOCUMENTS

Transparency is a core principle of the EDPB. As an EU body, the EDPB is subject to Art. 15 of the Treaty of the Functioning of the European Union and Regulation 1049/2001 on public access to documents. Art. 76(2) GDPR and Art. 32 of the EDPB's Rules of Procedure reinforce this requirement. The principle of transparency provides any EU citizen, and any natural or legal person residing or having a registered office in a Member State, with the right of access to EDPB documents. This right applies to all documents held by the EDPB, concerning any matter relating to its responsibilities. In exceptional cases, the EDPB may refuse to disclose all or part of a document. The reasons for such a refusal and corresponding procedural rules are outlined in Regulation 1049/2001 on public access to documents. In 2022, the EDPB

received 68 public access requests for documents held by the EDPB. Confirmatory applications were received in 7 cases<sup>1</sup>. In accordance with Art. 32(2) of the EDPB Rules of Procedure, the EDPB Secretariat prepares the answers to those requests, which are handled and signed by the Chair of the EDPB (for confirmatory applications) or one of the Deputy Chairs of the EDPB (for initial applications).

Three complaints regarding three EDPB's confirmatory decisions for requests for access to documents, submitted in 2021 and 2022, were brought to the attention of the European Ombudsman in 2022. Whilst the scope of the three complaints varied, their subject matter related to the US Foreign Account Tax Compliance Act (FATCA) and covered draft and final versions of statements, guidelines and letters, as well as correspondence. Following a reassessment of the requested documents, the EDPB decided to grant wider partial access to three documents, which were provided to the complainants. However, the EDPB informed the Ombudsman that access to most documents, mainly drafts, could not be granted in scope of these complaints, as several exceptions of Regulation 1049/2001 applied. Disclosure would have undermined the protection of privacy and the integrity of the individual (Art. 4(1)(b)) as well as the protection of the decision-making process at the EDPB (Art. 4(3)(2)). In particular, the EDPB argued that disclosing the draft documents would seriously jeopardize the EDPB's decision-making process, since the views of the EDPB members conveyed in the documents were at the time unknown to the public. The EDPB maintained that keeping the drafts from the general public is required for legal certainty, to avoid any confusion for stakeholders, as well as to ensure the consistent interpretation of EU data protection rules across the EU, and safeguard the EDPB's authority, independence and "space to think".

## 4.5. THE EDPB SECRETARIAT'S DATA PROTECTION OFFICER ACTIVITIES

The EDPB processes personal data following Regulation 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 (Regulation 2018/1725). In accordance with Art. 43 of Regulation 2018/1725, the EDPB designated its own DPO team, which is part of the EDPB Secretariat, to handle the processing of personal data. The DPO's position and tasks are defined in Arts. 44 and 45 of Regulation 2018/1725, and are further detailed in the [EDPB DPO Implementing Rules](#).

In 2022, the EDPB, with the assistance of its DPO team, continued to strengthen compliance with Regulation 2018/1725 by enhancing its transparency practices through different means, such as:

- development, publication and update of several privacy notices;
- continued development of several records, as well as publication of a centralised register for records on the EDPB website; and
- addition of new and updated information to its DPO website page.

The DPO team launched internal legal assessments on different issues concerning the EDPB's processing of personal data and identified suitable legal, organisational and, where applicable, technical solutions. The assessments were carried out as part of the DPO's advising function for the EDPB.

---

<sup>1</sup> According to Arts. 7 and 8 of the Regulation 1049/2001, when an application for access to documents is fully or partially refused, the applicant can file a confirmatory application, asking the institution to reconsider its position, within 15 working days (or as an exception, in 30 working days when the application relates to a long document or a large number of documents).

In 2022, the DPO team assisted with the handling of 6 data subject requests made on the basis of rights laid out in Art. 17 to Art. 24 of Regulation 2018/1725, which is the same figure as in 2021. The DPO team also provided assistance with replying to individual requests for information involving the processing of their personal data. In addition, the DPO team provided support in handling 12 data breaches under Arts. 34 and 35 of Regulation 2018/1725. The assessment of these data breaches revealed that a large majority of them was unlikely to pose a risk to the rights and freedoms of natural persons. Two data breaches required a notification to the EDPS.

Additionally, the DPO team delivered various internal training sessions and updated awareness-raising material aimed at EDPB Secretariat staff. These activities were tailored to the needs and expertise of the participants to ensure that all staff members were adequately informed of their responsibilities surrounding personal data processing, but also of their rights as data subjects.

Finally, the EDPB DPO team continued to maintain close relations with other EU institutions, bodies and agencies and their DPOs, particularly in matters involving or related to the processing of personal data. Such cooperation ensures the exchange of good practices, common experiences and tailored approaches to specific data protection challenges. To this end, the DPO team participated in the EU institutions' network of DPOs and the EDPB network of DPOs, comprising the DPOs of national SAs, the EDPS and the EDPB.



# 5

## EUROPEAN DATA PROTECTION BOARD - ACTIVITIES IN 2022

### 5.1. BINDING DECISIONS

#### 5.1.1. DECISION 01/2022 ON THE DRAFT DECISION OF THE FRENCH SUPERVISORY AUTHORITY REGARDING ACCOR SA UNDER ART. 65(1)(A) GDPR

*See Section 3.2.1. for the full summary.*

In June 2022, the EDPB resolved a dispute over a fine levied against the French hospitality company Accor SA. Initially, the French Lead Supervisory Authority (LSA) issued a draft decision against Accor SA, following the submission of complaints relating to difficulties when exercising the right to object to the receipt of marketing messages by email, and when exercising the right of access. The Polish SA voiced its objection to the

decision as it considered the amount of the fine not to be sufficiently effective, proportionate and dissuasive.

Following the SAs' failure to reach consensus, the case was referred to the EDPB pursuant to Art. 65(1) GDPR. The EDPB agreed with the Polish SA's reasoning in certain aspects. Among others, it decided that the French LSA needed to reassess the elements it relied upon to calculate the amount of the fine in order to ensure that it meets the criterion of dissuasiveness.

Following the binding decision of the EDPB, the French SA imposed a fine of EUR 500,000 for infringements relating to the GDPR. In addition, the French SA imposed a fine of EUR 100,000 for infringements of the national transposition of the ePrivacy directive.

Adopted: 15 June 2022

**5.1.2. BINDING DECISION 2/2022 ON THE DRAFT DECISION OF THE IRISH SUPERVISORY AUTHORITY REGARDING META PLATFORMS IRELAND LIMITED (INSTAGRAM) UNDER ART. 65(1)(A) GDPR**

*See Section 3.2.2. for the full summary.*

In July 2022, the EDPB resolved a dispute regarding the Irish SA's draft decision on Instagram, a service of Meta Platforms Ireland Limited (Meta IE). Several SAs voiced their objection to the decision, and following the failure to reach consensus, the case was referred to the EDPB pursuant to Art. 65(1) GDPR.

In terms of publicly disclosing children's emails and/or phone numbers when they operate Instagram business accounts, the EDPB held that Meta IE could not rely on Art. 6(1)(b) GDPR (performance of a contract) or Art. 6(1)(f) GDPR (legitimate interests) and concluded that Meta IE infringed Art. 6(1) GDPR by processing children's personal data in an unlawful manner. The EDPB further requested the Irish SA to reassess its determination of the administrative fine in this case.

Following the EDPB's decision, the Irish SA issued a EUR 405 million fine to Meta IE, which at the time of writing was the second highest fine issued by an SA since the adoption of the GDPR.

Adopted: 28 July 2022

**5.1.3. BINDING DECISION 3/2022 ON THE DISPUTE SUBMITTED BY THE IRISH SA ON META PLATFORMS IRELAND LIMITED AND ITS FACEBOOK SERVICE (ART. 65 GDPR) AND BINDING DECISION 4/2022 ON THE DISPUTE SUBMITTED BY THE IRISH SA ON META PLATFORMS IRELAND LIMITED AND ITS INSTAGRAM SERVICE (ART. 65 GDPR)**

*See Section 3.2.3. for the full summary.*

The EDPB adopted the [binding dispute resolution decisions](#) on 5 December 2022, after the Irish SA as LSA had triggered two dispute resolution procedures concerning the objections raised by several Concerned Supervisory Authorities (CSAs) about the processing activities carried out by Meta IE in the context of the Facebook and Instagram services.

In its decisions, the EDPB affirmed that Meta IE inappropriately relied on contract as a legal basis to process personal data in the context of Facebook's Terms of Service and Instagram's Terms of Use for the purpose of behavioural advertising. Thereby, the EDPB found that Meta IE lacked a legal basis for this processing and instructed the Irish SA to order Meta IE to bring its processing into compliance with Art. 6(1) GDPR.

In addition, EDPB noted that the grave breaches of transparency obligations impacted the reasonable expectations of the users, that Meta IE had presented its services to users in a misleading manner, and that the relationship between Meta IE and users of Facebook and Instagram services was imbalanced.

The EDPB directed the Irish SA to impose an administrative fine for the additional infringements of Art. 6(1) GDPR (lack of legal basis for the processing of personal data) and to issue significantly higher fines for the transparency infringements. Following the decisions, Meta IE was issued hefty fines by the Irish SA.

Adopted: 5 December 2022

#### **5.1.4. BINDING DECISION 5/2022 ON THE DISPUTE SUBMITTED BY THE IRISH SA REGARDING WHATSAPP IRELAND LIMITED (ART. 65 GDPR)**

*See Section 3.2.4. for the full summary.*

In December 2022, the EDPB adopted a binding decision that requested the Irish SA to amend its draft decision regarding WhatsApp Ireland Limited (WhatsApp IE) with respect to the findings concerning the lawfulness of the processing and the principle of fairness, and to the corrective measures envisaged.

According to the EDPB, WhatsApp IE inappropriately relied on contract as a legal basis to lawfully process personal data for Service improvement purposes. The Irish SA was thereby instructed to add an infringement of Art. 6(1) GDPR, as well as to include an infringement of the principle of fairness under Art. 5(1)(a) GDPR.

Furthermore, the EDPB requested that the Irish SA carries out an investigation into WhatsApp IE's processing operations in order to determine whether it processes special categories of personal data (Art. 9 GDPR); whether it processes data for the purposes of behavioural advertising, for marketing purposes, as well as for the provision of metrics to third parties and the exchange of data with affiliated companies for the purposes of service improvements.

Following the binding dispute resolution decision, the Irish SA issued a EUR 5.5 million fine to WhatsApp IE.

Adopted: 5 December 2022

## **5.2. CONSISTENCY OPINIONS**

### **5.2.1. OPINIONS ON DRAFT DECISIONS REGARDING BINDING CORPORATE RULES**

SAs may approve Binding Corporate Rules (BCRs) within the meaning of Art. 47 GDPR.

BCRs are data protection policies implemented and adhered to within a group of enterprises established in the EEA for transfers of personal data outside the EEA within the same group. In 2022, several SAs submitted their draft decisions regarding the controller or processor BCRs of various companies to the EDPB, requesting an Opinion under Art. 64(1)(f) GDPR. The EDPB issued twenty-three opinions on BCRs.

In all instances, the EDPB concluded that the draft BCRs contained all required elements and guaranteed appropriate safeguards to ensure that the level of protection provided by the GDPR would not be undermined when personal data was transferred to and processed by the group members based in third countries. It is without prejudice to the obligation of the data exporter to assess whether, in the specific case, additional measures are necessary to ensure an essentially equivalent level of protection to that in the EU. In every case, based on the EDPB Opinions, the BCRs could be approved without changes by the relevant SAs.

The various opinions are listed below:

- Opinion 02/2022 on the draft decision of the French Supervisory Authority regarding the Controller Binding Corporate Rules of the WEBHELP Group Adopted: 7 February 2022;

- Opinion 03/2022 on the draft decision of the French Supervisory Authority regarding the Processor Binding Corporate Rules of the WEBHELP Group Adopted: 7 February 2022;
- Opinion 04/2022 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of Norican Group Adopted: 18 March 2022;
- Opinion 05/2022 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of the Lundbeck Group Adopted: 19 April 2022;
- Opinion 06/2022 on the draft decision of the Irish Supervisory Authority regarding the Controller Binding Corporate Rules of Groupon International Limited Adopted: 19 April 2022;
- Opinion 07/2022 on the draft decision of the Hungarian Supervisory Authority regarding the Controller Binding Corporate Rules of MOL Group Adopted: 19 April 2022;
- Opinion 08/2022 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of Bioclinica Group Adopted: 4 May 2022;
- Opinion 09/2022 on the draft decision of the Danish Supervisory Authority regarding the Processor Binding Corporate Rules of Bioclinica Group Adopted: 4 May 2022;
- Opinion 10/2022 on the draft decision of the Hesse Supervisory Authority (Germany) regarding the Controller Binding Corporate Rules of Fresenius Group Adopted: 16 June 2022;
- Opinion 17/2022 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of the ANTOLIN Group Adopted: 1 August 2022;
- Opinion 18/2022 on the draft decision of the Baden-Württemberg (Germany) Supervisory Authority regarding the Controller Binding Corporate Rules of the Daimler Truck Group Adopted: 26 August 2022;
- Opinion 19/2022 on the draft decision of the Baden-Württemberg (Germany) Supervisory Authority regarding the Controller Binding Corporate Rules of the Mercedes-Benz Group Adopted: 26 August 2022;
- Opinion 20/2022 on the draft decision of the Irish Supervisory Authority regarding the Controller Binding Corporate Rules of the Ellucian Group Adopted: 26 August 2022;
- Opinion 21/2022 on the draft decision of the Irish Supervisory Authority regarding the Processor Binding Corporate Rules of the Ellucian Group Adopted: 26 August 2022;
- Opinion 22/2022 on the draft decision of the Liechtenstein Supervisory Authority regarding the Controller Binding Corporate Rules of Hilti Group Adopted: 7 September 2022;
- Opinion 23/2022 on the draft decision of the Swedish Supervisory Authority regarding the Controller Binding Corporate Rules of the Samres Group Adopted: 7 September 2022;
- Opinion 24/2022 on the draft decision of the Swedish Supervisory Authority regarding the Processor Binding Corporate Rules of the Samres Group Adopted: 7 September 2022;
- Opinion 26/2022 on the draft decision of the Data Protection Authority of Bavaria for the Private Sector regarding the Controller Binding Corporate Rules of the Munich Re Reinsurance Group Adopted: 30 September 2022;

- Opinion 27/2022 on the draft decision of the French Supervisory Authority regarding the Processor Binding Corporate Rules of LEYTON Group Adopted: 7 October 2022;
- Opinion 29/2022 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of the DSV Group Adopted: 18 November 2022;
- Opinion 30/2022 on the draft decision of the Slovak Supervisory Authority regarding the Controller Binding Corporate Rules of the Piano Group Adopted: 28 November 2022;
- Opinion 31/2022 on the draft decision of the Slovak Supervisory Authority regarding the Processor Binding Corporate Rules of the Piano Group Adopted: 28 November 2022;
- Opinion 32/2022 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of the Ramboll Group Adopted: 06 December 2022.

### **5.2.2. OPINIONS ON DRAFT REQUIREMENTS FOR ACCREDITATION OF A CERTIFICATION BODY**

Three SAs submitted their draft decisions on accreditation requirements for certification bodies under Art. 43(1)(b) GDPR to the EDPB, requesting an opinion under Art. 64(1)(c) GDPR. These requirements allow the accreditation of certification bodies responsible for issuing and renewing certification in accordance with Art. 42 GDPR.

These opinions aim to establish a consistent and harmonised approach regarding the requirements that SAs and national accreditation bodies apply when accrediting certification bodies under the GDPR. To do so, the EDPB made recommendations to the relevant SAs on the amendments to be made to the draft

accreditation requirements. The SAs then amended their drafts in accordance with Art. 64(7) GDPR, taking utmost account of the opinions of the EDPB.

The various opinions are listed below:

- Opinion 11/2022 on the draft decision of the competent Supervisory Authority of Poland regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43.3 (GDPR) Adopted: 4 July 2022;
- Opinion 12/2022 on the draft decision of the competent Supervisory Authority of France regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43.3 (GDPR) Adopted: 4 July 2022;
- Opinion 13/2022 on the draft decision of the competent Supervisory Authority of Bulgaria regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43.3 (GDPR) Adopted: 4 July 2022.

### **5.2.3. OPINIONS ON CERTIFICATION CRITERIA**

When an SA intends to approve a certification pursuant to Art. 42(5) GDPR, the main role of the EDPB is to ensure the consistent application of the GDPR through the consistency mechanism referred to in Arts. 63, 64 and 65 GDPR. Under this framework, according to Art. 64(1)(c) GDPR, the EDPB is required to issue an opinion on an SA's draft decision approving the certification criteria. The EDPB issued three opinions on certification criteria in 2022, aiming at ensuring the consistent application of the GDPR, including by the SAs, controllers and processors.

The three opinions are listed below:

- Opinion 1/2022 on the draft decision of the Luxembourg Supervisory Authority regarding the GDPR – CARPA certification criteria Adopted: 8 February 2022;

- Opinion 25/2022 regarding the European Privacy Seal (EuroPriSe) certification criteria for the certification of processing operations by processors Adopted: 22 September 2022;
- 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) Adopted: 10 October 2022.

#### **5.2.4. OPINIONS ON SAS' APPROVAL OF ACCREDITATION REQUIREMENTS FOR CODE OF CONDUCT MONITORING BODY**

The EDPB issued three opinions on draft accreditation requirements for code of conduct monitoring bodies, as requested by SAs in accordance with Art. 64(1)(c) GDPR.

The aim of these EDPB opinions is to ensure consistency and the correct application of the requirements among SAs. To do so, the EDPB made several recommendations to the various SAs on the amendments to be made to the draft accreditation requirements. On this basis, the SAs amended their drafts in accordance with Art. 64(7) GDPR, taking utmost account of the opinions of the EDPB.

The various opinions are listed below:

- Opinion 14/2022 on the draft decision of the competent Supervisory Authority of Bulgaria regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR Adopted: 4 July 2022;
- Opinion 15/2022 on the draft decision of the competent Supervisory Authority of Luxembourg regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR Adopted: 4 July 2022;

- Opinion 16/2022 on the draft decision of the competent Supervisory Authority of Slovenia regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted: 4 July 2022.

## **5.3. GENERAL GUIDANCE**

### **5.3.1. GUIDELINES 01/2022 ON DATA SUBJECT RIGHTS - RIGHT OF ACCESS**

The guidelines provide further clarity on the right of access, a cornerstone right of data subjects that is enshrined in Art. 8 of the EU Charter of Fundamental Rights. It has been a part of the European data protection framework since its beginning and has been further developed by more precise rules in Art. 15 GDPR.

With the exceptions referred to in the GDPR and analysed in the guidelines, the right of access allows data subjects to obtain full disclosure of their personal data. Unless explicitly stated otherwise, the request should be understood as referring to all personal data concerning the data subject. The right of access includes three different components:

- i. confirmation as to whether data about the person is processed or not;
- ii. access to this personal data; and
- iii. 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.

The guidelines provide clarifications on the scope of the right of access, the information the controller has to provide to the data subject, the format of the access request, the main modalities for providing access and the limits and restrictions of the right. The controller

may ask the data subject to specify the request if they process a large amount of data. Even data that may be incorrect or unlawfully processed will have to be provided. At the same time, the guidelines elaborate on the limits and restrictions of the right. The guidelines provide examples to support controllers in answering access requests in a GDPR-compliant manner.

Adopted: 18 January 2022

### **5.3.2. GUIDELINES 02/2022 ON THE APPLICATION OF ART. 60 GDPR**

*See Section 3.1.2. for the full summary.*

The EDPB adopted Guidelines 02/2022 with the aim of providing guidance on cooperation between SAs and on the One-Stop-Shop (OSS) mechanism. In practice, the guidelines help SAs to enact their own national procedures in a manner consistent with the cooperation under the OSS mechanism. The guidelines elaborate and clarify the requirements of each paragraph of Art. 60 GDPR, based on the provision's text and its practical implementation. Overall, the provided guidance significantly contributes to the desired consistency of the SAs' work and to enhancing enforcement cooperation.

Adopted: 14 March 2022

### **5.3.3. GUIDELINES 03/2022 ON DECEPTIVE DESIGN PATTERNS IN SOCIAL MEDIA PLATFORM INTERFACES: HOW TO RECOGNISE AND AVOID THEM**

The EDPB Guidelines 03/2022 aim to help designers and users of social media platforms in deciding how to assess and avoid deceptive design (so-called "dark patterns") that infringe on GDPR requirements. The Guidelines define dark patterns as "interfaces and user experiences implemented on social media platforms that lead users into making unintended, unwilling and

potentially harmful decisions regarding the processing of their personal data".

The categories of dark patterns addressed in the Guidelines are: a) overloading, b) skipping, c) stirring, d) hindering, e) fickle and f) left in the dark.

These Guidelines provide examples of deceptive design in use cases of the life cycle of a social media account (i.e. from the sign-up stage to the closing of a social media account).

In addition to the examples of deceptive design, the Guidelines include best practices at the end of each use case (i.e. specific recommendations for designing user interfaces that facilitate the effective implementation of the GDPR).

Adopted: 14 March 2022

### **5.3.4. GUIDELINES 04/2022 ON THE CALCULATION OF ADMINISTRATIVE FINES UNDER THE GDPR**

*See Section 3.1.3. for the full summary.*

The guidelines contribute to an important part of the EDPB's strategy based on creating more efficient cooperation among SAs on cross-border cases, by harmonising the approach used by SAs in calculating fines. The EDPB devised a systematic and chronological five-step methodology that SAs across the European Economic Area (EEA) can use for calculating administrative fines for infringements of the GDPR. The circumstances of the specific case are the determining factors leading to the final amount, which can – in all cases – vary between any minimum amount and the legal maximum.

Adopted: 12 May 2022

### **5.3.5. GUIDELINES 05/2022 ON THE USE OF FACIAL RECOGNITION TECHNOLOGY IN THE AREA OF LAW ENFORCEMENT**

Increasingly, law enforcement authorities (LEAs) are showing an interest in the use of facial recognition technology (FRT). This technology often relies on artificial intelligence (AI) or machine learning (ML) and can be used, for example, to search for persons on police watch lists or to monitor the movements of an individual in public space.

FRT relies on the processing of biometric data, which benefit from special protection in the legal framework. Indeed, biometric data are permanently and irrevocably linked to an individual's identity, and therefore carry significant data protection implications.

Through its guidelines, the EDPB outlines the applicable legal framework that lawmakers at the national and EU level, as well as LEAs using the FRT systems, must strictly comply with to ensure data subjects' rights.

The guidelines also provide a tool to support a first classification of a given use case (Annex I) as well as practical guidance for LEAs that plan to procure and run an FRT-system. Further, the guidelines include a set of hypothetical situations illustrating concrete uses of FRT and relevant considerations, especially regarding the necessity and proportionality test.

Adopted: 12 May 2022

### **5.3.6. GUIDELINES 06/2022 ON THE PRACTICAL IMPLEMENTATION OF AMICABLE SETTLEMENTS**

Through these guidelines, the EDPB discusses the power to reach an amicable settlement as well as the role of the amicable settlement in the context of the One-Stop-Shop mechanism. It analyses the legal consequences and includes practical

recommendations, proposing a step-by-step guide for handling a case via amicable settlement.

In the context of complaint handling by SAs, most Member States see amicable settlements as a process of "alternative dispute resolution". In most cases, the amicable settlement solution is relied on where a complaint is lodged with the SA concerning an 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.

The EDPB recognises that amicable settlements are tools to achieve compliance with the GDPR by the controller. In case a complaint is lodged because a controller has not fulfilled the data subject rights pursuant to Art. 12 to Art. 22 GDPR, the enforcement of data subject rights can be expedited by an amicable arrangement between the actors.

Adopted: 18 November 2021; formatting changes made on 12 May 2022

### **5.3.7. GUIDELINES 07/2022 ON CERTIFICATION AS TOOL FOR TRANSFERS**

In its Art. 46, the GDPR requires data exporters to put in place appropriate safeguards for transfers of personal data to third countries or international organisations. To that end, the GDPR distinguishes appropriate safeguards that may be used by data exporters under Art. 46 for framing transfers to third countries by introducing, amongst others, certification as a new transfer mechanism (Arts. 42(2) and 46(2)(f) GDPR).

These guidelines provide guidance on the application of Art. 46(2)(f) GDPR regarding transfers of personal data to third countries or to international organisations on the basis of certification.

First, the EDPB underlines that the nature of these guidelines is complementary to the general Guidelines 1/2018 on certification. The guidelines specify the requirements for transfers under GDPR when certification is used. In this respect, the EDPB clarifies the obligations of the data exporter and the data importer, with a special focus on the latter, who will be granted the certification.

In addition, the EDPB provides guidance on the certification criteria already listed in Guidelines 01/2018 and establishes additional specific criteria that should be included in a certification mechanism used as a tool for transfers to third countries, such as the assessment of the third country legislation, the rules on onward transfers and redress and enforcement. Lastly, the guidelines discuss the elements that should be addressed in the binding and enforceable commitments that controllers or processors not subject to the GDPR should take in order to provide appropriate safeguards for data transferred to third countries.

Adopted: 14 June 2022

### **5.3.8. GUIDELINES 8/2022 ON IDENTIFYING A CONTROLLER OR PROCESSOR'S LSA**

These guidelines constitute a targeted update of the Article 29 Working Party's guidelines for identifying a controller or processor's LSA (paragraphs 29-34 and points I and III under 2.d. of the Annex), previously endorsed by EDPB. The document gives further clarifications on the notion of main establishment in the context of joint controllership and builds on the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

Adopted: 10 October 2022

### **5.3.9. GUIDELINES 9/2022 ON PERSONAL DATA BREACH NOTIFICATION UNDER GDPR**

The Article 29 Working Party guidelines on personal data breach notification under Regulation 2016/679 guidelines, previously endorsed by the EDPB, outline the mandatory breach notification and communications requirements of the GDPR and provide suggestions for how controllers and processors can fulfil these obligations. In the targeted update of these guidelines, the EDPB clarifies the notification requirements concerning personal data breaches at non-EU establishments. The updated guidelines specify that data controllers who are not established in the EU will need to notify data breaches to every single authority for which affected data subjects reside in their Member State. The mere presence of a representative in a Member State does not trigger the one-stop-shop system.

Adopted: 10 October 2022

### **5.3.10. GUIDELINES ADOPTED AFTER PUBLIC CONSULTATION**

#### **5.3.10.1. GUIDELINES 01/2021 ON EXAMPLES REGARDING PERSONAL DATA BREACH NOTIFICATION**

The EDPB adopted these practice-oriented and case-based guidelines to help data controllers in deciding how to handle personal data breaches and what factors to consider during risk assessment.

The guidelines address six categories of personal data breaches and outline several examples of typical situations based on the SAs' experience. The categories of personal data breaches addressed in the guidelines are as follows:

- 1. Ransomware attacks** which involve malicious code encrypting personal data, where the attacker requests a ransom in exchange for a decryption code.
- 2. Data exfiltration attacks** which exploit vulnerabilities in services offered over the internet and usually aim to copy, exfiltrate and abuse personal data for some malicious end.
- 3. Internal human-related risk source** which refers to human errors leading to personal data breaches, which can have a frequent occurrence and can be both deliberate or accidental, therefore making it difficult for data controllers to identify weaknesses and take steps to avoid them.
- 4. Loss or theft of devices and/or documents** which is a frequent occurrence of a data breach that might present a difficult risk assessment when devices are no longer available.
- 5. Mispostal** which involves internal human error in setting the recipient(s) of a communication. The error occurs due to inattentiveness without any malicious intention.
- 6. Social engineering** which refers to psychological manipulation attacks involving identity theft and email exfiltration.

For each category of personal data breaches the guidelines provide advisable, but not exclusive or comprehensive, practical measures to be considered both when dealing with data breaches and for future prevention.

Adopted: 14 January 2021 and adopted in its final version following public consultation on 14 December 2021

#### 5.3.10.2. GUIDELINES 04/2021 ON CODES OF CONDUCT AS TOOLS FOR TRANSFERS

In accordance with Art. 46 GDPR, controllers and processors shall put in place appropriate safeguards for transfers of personal data to third countries or international organisations. Therefore, the GDPR

distinguishes the appropriate safeguards that may be used by organisations under Art. 46 for framing transfers to third countries by introducing, amongst others, codes of conduct as a new transfer mechanism (Arts. 40(3) and 46(2)(e) GDPR). Controllers and processors are required to make binding and enforceable commitments, via contractual or other legally binding instruments, to apply the appropriate safeguards.

In the guidelines, the EDPB underlines that, in terms of content, such codes should address the essential principles, rights and obligations arising under the GDPR for controllers and processors and include guarantees that are specific to the context of transfers, such as onward transfers or conflict of laws in the third country. Striving towards a practical implementation of the guidelines, the EDPB provides a checklist of the elements to be covered.

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 displayed through flow charts.

Adopted: 7 July 2021; formatting changes made on 22 February 2022

#### 5.4. REGISTER FOR DECISIONS TAKEN BY SA AND COURTS ON ISSUES HANDLED IN THE CONSISTENCY MECHANISM

The EDPB maintains a publicly accessible electronic [register of decisions](#) taken by SAs and courts on issues handled in the consistency mechanism per Art. 70(1) (y) GDPR. This register provides for accessibility and transparency of the decisions and further promotes the consistent application of the GDPR by the European SAs.

All decisions added in 2022 are related to decisions made by the SAs following the EDPB consistency opinions or following the 01/2022 EDPB binding decision on the dispute arisen on the draft decision of the French SA regarding Accor SA.

See Section 5.2 on consistency opinions and Section 5.1 on binding decisions.

### **5.5. LEGISLATIVE CONSULTATION AND DOCUMENTS ADDRESSED TO THE EU INSTITUTIONS OR NATIONAL AUTHORITIES**

#### **5.5.1. EDPS-EDPB JOINT OPINION 1/2022 ON THE EXTENSION OF THE COVID-19 CERTIFICATE REGULATION**

On 3 February 2022, the European Commission adopted, firstly, a Proposal for a Regulation on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic for EU citizens, and secondly, a Proposal for a Regulation on the same matters, but applying to third-country nationals legally staying or residing in the territories of Member States.

As a general remark, the EDPB and the EDPS recall in their opinion that compliance with data protection rules does not constitute an obstacle to fighting the COVID-19 pandemic and that, at the same time, the general principles of effectiveness, necessity and proportionality must guide any measure adopted by Member States or EU institutions that involve the processing of personal data to fight COVID-19. In addition, the EDPB and the EDPS underline that any restriction to the free movement of persons within the European Union put in place to limit the spread of SARS-CoV-2, including the requirement to present EU Digital COVID Certificates, should be lifted as soon as the epidemiological situation allows.

The EDPS and EDPB take note that the European Commission did not carry out an impact assessment for the Proposals, due to the urgency and their limited scope. They strongly consider that the Proposals should be accompanied by an impact assessment report, in order to provide a clear justification on the necessity and proportionality, taking into account the evolution of the epidemiological situation with regard to the COVID-19 pandemic together with the impact on fundamental rights and non-discrimination.

Lastly, the EDPB and the EDPS invite the Commission to assist the Member States in developing technical specifications on the recognition of information about the COVID-19 vaccine and the number of doses administered to the holder, regardless of the Member State in which they have been administered.

Adopted: 14 March 2022

#### **5.5.2. EDPB-EDPS JOINT OPINION 2/2022 ON THE PROPOSAL OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON HARMONISED RULES ON FAIR ACCESS TO AND USE OF DATA (DATA ACT)**

In a joint effort, the EDPB and the EDPS comment on overarching concerns related to the [Proposal for the Data Act](#) and urge the co-legislator to take decisive action. While welcoming the efforts made to ensure that the Proposal does not affect the current data protection framework, the EDPB and the EDPS consider that additional safeguards are necessary to avoid lowering the protection of the fundamental rights to privacy and to the protection of personal data in practice. Their comments concern three distinct areas: i) the rights to access, use and share data, ii) the obligation to make data available in case of “exceptional need”, and iii) the implementation and enforcement.

First, the Joint Opinion stresses the need for provisions explicitly specifying that data protection law “prevails” in case of conflict with the provisions of the Proposal insofar as the processing of personal data is concerned. In addition, a more robust application of the data minimisation principle is encouraged when designing new products. Along with that, the Opinion calls for an enhancement of the right to data portability. In general, the EDPB and the EDPS stress the need to ensure that access, use, and sharing of personal data by users other than data subjects, as well as by third parties and data holders, should occur in full compliance with all of the provisions of the GDPR, EUDPR and ePrivacy Directive.

Second, the EDPB and the EDPS express concerns regarding the lawfulness, necessity and proportionality of the obligation to make data available to public sector bodies and EU institutions, agencies or bodies in case of “exceptional need”. They remind that any limitation of the right to protection of personal data must be based on a legal basis that is adequately accessible and foreseeable and formulated with sufficient precision to enable individuals to understand its scope.

Third, regarding implementation and enforcement, the EDPB and the EDPS highlight the risk of operational difficulties that might result from the designation of more than one competent authority responsible for the application and enforcement of the Proposal. At the same time, they welcome the designation of the data protection SAs as competent authorities responsible for monitoring the application of the Proposal insofar as the protection of personal data is concerned, and they ask the co-legislators to also designate national SAs as coordinating competent authorities under this Proposal.

Adopted: 4 May 2022

### **5.5.3. EDPB-EDPS JOINT OPINION 03/2022 ON THE PROPOSAL FOR A REGULATION ON THE EUROPEAN HEALTH DATA SPACE**

The EDPB and the EDPS jointly expressed their views on the proposed [Regulation on the European Health Data Space](#). The resulting opinion first notes that the Proposal aims at: i) supporting individuals to take control of their own health data, ii) supporting the use of health data for better healthcare delivery, better research, innovation and policy making, and iii) enabling the EU to make full use of the potential offered by a safe and secure exchange, use and reuse of health data. However, they are concerned that the Proposal may weaken the protection of the rights to privacy and to data protection, especially considering the categories of personal data and purposes that are related to the secondary use of data. They also note that the Proposal will add yet another layer to the already complex (multi-layered) collection of provisions (to be found both in the EU and Member States law) on the processing of health data (in the health care sector).

In that respect, the EDPB and the EDPS consider that it is important to clarify the relationship between the provisions in the Proposal with the ones in the GDPR and Member State laws. Additionally, with regards to the scope, they recommend excluding wellness applications and other digital applications, as well as wellness and behaviour data relevant to health. Should this be maintained, the EDPB and the EDPS suggest that personal data deriving from wellness apps and other digital health applications should not be included in the secondary use of health data, as they do not have the same data quality requirements and characteristics as those generated by medical devices. Further, they strongly recommend not extending the scope of the GDPR exceptions regarding the data subject’s rights and note the need to remain consistent with the relevant GDPR provisions.

The EDPB and the EDPS are of the view that the Proposal should further delineate purposes for secondary use and circumscribe when there is a sufficient connection with public health and/or social security.

Lastly, the EDPB and the EDPS acknowledge that the infrastructure for the exchange of electronic health data foreseen in the Proposal will not establish a central EU-database of health data and will only facilitate the exchange of such health data from decentralised databases. However, due to the large quantity of data that would be processed and their highly sensitive nature, among others, the EDPB and the EDPS call for a requirement for storing the personal electronic health data in the EU/EEA, without prejudice to further transfers in compliance with Chapter V of the GDPR.

Adopted: 12 July 2022

### **5.5.4. EDPB-EDPS JOINT OPINION 04/2022 ON THE PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN RULES TO PREVENT AND COMBAT CHILD SEXUAL ABUSE**

In relation to the European Commission's Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, the EDPB and the EDPS adopted a joint opinion on 28 July 2022. While emphasizing the gravity of child sexual abuse as a serious and heinous crime, the Opinion expresses serious concerns regarding the proportionality of the envisaged interference and limitations to the protection of the fundamental rights to privacy and the protection of personal data.

The EDPB and EDPS note that the Proposal's lack of detail, clarity, and precision regarding the conditions for issuing a detection order for child sexual abuse

material (CSAM) and child solicitation does not ensure that only targeted approaches to detecting CSAM are used. They raise the concern that the Proposal could potentially be used as a basis for generalised and indiscriminate scanning of the content of all types of electronic communications. As a result, the EDPB and EDPS recommend that the conditions for issuing detection orders be further clarified to address these concerns.

Additionally, the EDPB and EDPS raise concerns about the measures envisaged for the detection of unknown CSAM and the solicitation of children in interpersonal communication services, in particular due to likelihood of errors and their high level of intrusiveness into the privacy of individuals. Overall, the EDPB and the EDPS argue that the requirement imposed on online service providers to decrypt online communications in order to block those related to CSAM is disproportionate to the aim pursued.

The EDPB and EDPS underline that breaking or weakening encryption in order to access private communications would have a substantial impact on the right to private life and to the confidentiality of communications, freedom of expression, innovation and growth of the digital economy.

Lastly, the EDPB and EDPS recommend that the relationship between the tasks of the national Coordinating Authorities under the Proposal and SAs be better regulated. They also underline that the transmission of personal data between the newly proposed EU Centre and Europol should only take place following a duly assessed request case-by-case.

Adopted: 28 July 2022

### 5.5.5. STATEMENT 01/2022 ON THE ANNOUNCEMENT OF AN AGREEMENT IN PRINCIPLE ON A NEW TRANS-ATLANTIC DATA PRIVACY FRAMEWORK

The GDPR requires that the European Commission seeks an opinion of the EDPB before adopting a possible new adequacy decision recognising as satisfactory the level of data protection guaranteed by a third country. In principle, the EDPB welcomes the announcement of a political agreement between the European Commission and the United States on 25 March 2022 on a new Trans-Atlantic Data Privacy Framework. This announcement is made at a time when transfers from the EEA to the U.S. face significant challenges.

The EDPB looks forward to carefully assessing the improvements that a new Trans-Atlantic Data Privacy Framework may bring in light of the EU law, the case law of the CJEU and the recommendations EDPB made on that basis. In particular, the EDPB will analyse in detail how these reforms ensure that the collection of personal data for national security purposes is limited to what is strictly necessary and proportionate.

Lastly, the EDPB will examine to what extent the announced independent redress mechanism respects the EEA individuals' right to an effective remedy and to a fair trial. In particular, the EDPB will look at whether any new authority involved in this mechanism has access to relevant information, including personal data, when exercising its mission and can adopt decisions binding on the intelligence services, and whether there is a judicial remedy against this authority's decisions or inaction.

Adopted: 6 April 2022

### 5.5.6. STATEMENT 04/2022 ON THE DESIGN CHOICES FOR A DIGITAL EURO FROM THE PRIVACY AND DATA PROTECTION PERSPECTIVE

In its Statement, the EDPB emphasises the importance of ensuring a very high standard of privacy and data protection by design and by default in the digital euro project. To meet this standard, the EDPB suggests that different design choices should be considered and adopted based on a documented impact assessment prioritising innovative and privacy-enhancing technologies.

The EDPB cautions against the use of systematic validation and tracing of all transactions in digital euro. In this regard, the EDPB advises that the digital euro be made available both online and offline, along a threshold below which no tracing is possible, in order to guarantee full anonymity of daily transactions.

The EDPB also welcomes the European Commission's intention to propose in 2023 a specific legal framework for the digital euro, for which it stands ready to provide relevant guidance. Finally, the EDPB urges the European Central Bank and the European Commission to enhance public debate on the digital euro project to ensure it meets the highest standards of privacy and data protection.

Adopted: 10 October 2022

### 5.5.7. RESPONSE OF THE EDPB TO THE EUROPEAN COMMISSION'S TARGETED CONSULTATION ON A DIGITAL EURO

In April 2022, the European Commission launched a public consultation to gather information on the expected impact of the digital euro on stakeholders, including with regard to its privacy and data protection aspects.

In its contribution to this consultation, the EDPB recalls the views it expressed to the European institutions in a letter of June 2021, namely that a high level of data protection and privacy rights is crucial to strengthen end-users' trust in the digital euro project, and thus to ensure its acceptance by European citizens. In order to achieve this, the EDPB recommends that the features of the digital euro be designed as closely as possible to physical cash.

In particular, the EDPB stresses the importance of providing individuals with a bearer-based architecture available both online and offline. Furthermore, the EDPB is of the opinion that controls of transactions should only be carried out by the competent authorities and reduced to the minimum necessary. Finally, the EDPB recommends that such transactions should not be traceable at all below a certain threshold.

Adopted: 14 June 2022

## **5.5.8. STATEMENT ON THE IMPLICATIONS OF THE CJEU JUDGMENT C-817/19 ON THE USE OF PNR IN MEMBER STATES**

Following the CJEU judgment on the Directive (EU) 2016/681 (also referred to as the "PNR Directive") on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, the EDPB adopted a Statement on 13 December 2022.

In its ruling, the CJEU set out strict limitations which must be observed by a Member State when transposing and applying the PNR Directive. The limitations that stand out as the most relevant ones are:

- limitation to the purposes set out in the PNR Directive, which are exhaustive;

- application of the PNR system only to terrorist offences and serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air and thus also exclusion of ordinary crime;
- limitation of the application of the PNR Directive with regard to intra-EU flights and other means of transport; and
- no indiscriminate application of the general retention period of five years to all air passengers' personal data.

In response to the judgment, the EDPB, through its Statement, asked Member States to take all necessary steps to guarantee that their national implementations of the PNR Directive are in line with the fundamental right to the protection of personal data, as laid down in Art. 8 of the EU Charter of Fundamental Rights. Steps taken by the Member States must include legislative measures as well as the identification of measures that can be adopted promptly in practice.

Adopted: 13 December 2022

## **5.6. OTHER GUIDANCE AND INFORMATION NOTES**

### **5.6.1. STATEMENT 02/2022 ON PERSONAL DATA TRANSFERS TO THE RUSSIAN FEDERATION**

Recent geopolitical developments had Russia excluded from the Council of Europe on 16 March 2022. Although Russia continues to be a contracting party to conventions and protocols concluded in the framework of the Council of Europe to which it has expressed its consent to be bound, for instance, Convention 108, the modalities of Russia's participation in these instruments are still to be determined.

In its Statement, the EDPB recalls that the transfer of personal data to a third country, in the absence of

an adequacy decision of the European Commission pursuant to Art. 45 GDPR, is only possible if the controller or processor has provided appropriate safeguards, and on condition that enforceable rights and effective legal remedies are available for data subjects (Art. 46 GDPR), or in specific circumstances, only on one of the conditions set forth in Art. 49 GDPR.

Russia does not benefit from an adequacy finding by the European Commission in accordance with Art. 45 GDPR. Therefore, the EDPB notes that, when personal data are transferred to Russia, data exporters under the GDPR should assess and identify the legal basis for the transfer and the instrument to be used among those provided by Chapter V GDPR (e.g., Standard Contractual Clauses or Binding Corporate Rules), in order to ensure the application of appropriate safeguards.

SAs of EEA Member States which have close economic and historic ties with Russia are already looking into the lawfulness of data transfers to Russia, including in the context of ongoing investigations. They will handle cases involving data transfers to Russia, taking into account the increased impact on the rights and freedoms of data subjects that may arise from such data processing operations, and will coordinate within the EDPB, as appropriate.

Adopted: 12 July 2022

## 5.7. GDPR COOPERATION AND ENFORCEMENT

### 5.7.1. STATEMENT ON ENFORCEMENT COOPERATION

On 28 April 2022, the EDPB adopted a [Statement on enforcement cooperation](#), following a high-level meeting in Vienna where EDPB members agreed to enhance cooperation on strategic cases and to diversify the range of cooperation methods used.

The Statement recalls the SAs' commitment to close cross-border cooperation. The SAs agree to collectively and regularly identify cross-border cases of strategic importance, with the EDPB's support, in different Member States. Additionally, SAs commit to further exchanging information on national enforcement strategies in order to reach an agreement on annual enforcement priorities at the EDPB level.

The Statement also reiterates the EDPB's role in ensuring a consistent interpretation of the GDPR. The EDPB shall deal with specific legal issues on matters of general application as well as facilitate the cross-border exchange of information. Lastly, in order to maximise the positive impact of GDPR cooperation, the EDPB set out to identify a list of procedural aspects that can be further harmonised in EU law.

For more on the Statement on enforcement cooperation see [Section 3.1.1](#).

Adopted: 28 April 2022

### 5.7.2. EDPB DOCUMENT ON THE SELECTION OF CASES OF STRATEGIC IMPORTANCE

Following the Vienna meeting of April 2022, the EDPB adopted a document that establishes criteria for determining whether a case is of strategic importance, in line with the [Statement on enforcement cooperation](#). The EDPB considers cases to be of strategic importance if there is a high risk to the rights and freedoms of natural persons in several Member States.

Pursuant to the document, a proposal voluntarily submitted by an SA may qualify as a case of strategic importance if it concerns a structural or recurring problem in several Member States, is related to the intersection of data protection with other legal fields, and/or affects a large number of data subjects in several Member States. Cases that involve a large

number of complaints in several Member States, a fundamental issue falling within the scope of the EDPB strategy, and/or matters where the GDPR implies that high risk can be assumed, also qualify as strategically important cases.

Further, the EDPB lays down in its document the process and timeline for the selection of cases. A template for the proposal of a strategic case is also provided by the EDPB, to ensure that Member States include all the information relevant to the case when submitting their proposal.

### **5.7.3. COORDINATED ENFORCEMENT FRAMEWORK**

Ever since the implementation of the GDPR, the EDPB has emphasised the importance of consistent enforcement through cooperation efforts. Hence, in line with its 2021-2023 Strategy, the EDPB set up a [Coordinated Enforcement Framework \(CEF\)](#), which provides a structure for recurring annual coordinated action by SAs. The CEF works to facilitate joint actions in a coordinated and flexible manner, including activities such as joint awareness campaigns, information gathering, enforcement sweeps as well as joint investigations. Annual coordinated efforts are intended to improve compliance, empower individuals to exercise their rights and increase awareness of data protection issues.

In 2022, the EDPB considerably increased its efforts to streamline enforcement cooperation, particularly through various initiatives focused on improving cooperation among SAs. During the year, as a result of effective cooperation, EDPB members launched their first coordinated action on the use of Cloud-based services by the public sector.

For more on enforcement cooperation, [see Section 3.1](#).

### **5.7.4. SUPPORT POOL OF EXPERTS**

As part of its 2021-2023 Strategy, the EDPB established a Support Pool of Experts (SPE) in 2020. The SPE's main objective is to assist SAs in carrying out investigations and enforcement activities of significant common interest. The SPE provides support in the form of expertise for investigations and enforcement activities of common interest to SAs and enhances cooperation/solidarity by reinforcing and complementing the strengths of the individual SAs and addressing operational needs. This includes but is not limited to, analytical support, assistance in the performance findings of a forensic nature, as well as in the preparation of investigative reports on the basis of evidence collected. Further, the SPE enhances the cooperation and solidarity between all EDPB members by sharing, reinforcing and complementing strengths and addressing operational needs.

A call for external experts was launched and at the end of 2022, the SPE was composed of 409 external experts.

## **5.8. PLENARY MEETINGS AND SUBGROUPS**

In the period between 1 January and 31 December 2022, the EDPB held 15 plenary meetings.

The agendas and minutes of these meetings are published on the EDPB website. The outcome of the plenary meetings consists of adopted guidelines, opinions and other documents such as statements or information notes to advise the European Commission, national SAs and other stakeholders on data protection matters, with a primary focus on the GDPR. Additionally, there were 160 expert subgroup meetings and 172 drafting team meetings. In total, 347 meetings were held, including plenary meetings, expert subgroup meetings, task force meetings and drafting team meetings.

The different expert subgroups focus on specific areas of data protection and assist the EDPB in performing its tasks. Chapter 9 outlines the list of the expert subgroups and their respective mandates.

## 5.9. STAKEHOLDER CONSULTATION

### 5.9.1. STAKEHOLDER EVENTS

The EDPB invited various NGOs to the 69th Plenary meeting to discuss challenges caused by differences in national administrative law. Participants acknowledged the importance of the Vienna meeting and the [EDPB statement on enforcement cooperation](#). They indicated that a significant number of the issues they faced with the One-Stop-Shop were caused by differences in national procedural law. The NGO representatives notably discussed the procedural issues faced when lodging complaints. Constructive criticism was given in the context of the SAs' duty to decide on a complaint, specifically regarding the lack of information they provide to the complainants.

The NGOs stressed that in order to ensure the right to a legal remedy, every complaint must lead to a formal decision. They further advocated for clear deadlines for each step of the cooperation procedure and identified issues related to the informal closing or narrowing down the scope of complaints. Additionally, the NGOs addressed, among others, the notification of decisions. Finally, the NGOs stated that reopening the GDPR at this stage was unnecessary.

### 5.9.2. PUBLIC CONSULTATION ON DRAFT GUIDANCE

Following the preliminary adoption of guidelines, the EDPB organises public consultations to give stakeholders and citizens the opportunity to provide additional input. The EDPB Members and the EDPB Secretariat in charge of drafting the guidelines consider this input before adopting the guidelines in their final version.

To increase transparency, the stakeholders' contributions to public consultations are published by the EDPB on its website. In 2022, the EDPB launched several consultations:

- In January, the EDPB opened public consultations on [Guidelines 01/2022 on data subject rights – Right of access](#). There were 72 contributions made to the guidelines from a mix of entities such as business associations, NGOs, companies, research institutions and consumer organisations. Natural persons also contributed to the public consultation.
- In March, [Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them](#) were open for public consultations. A total of 26 contributions were made to these guidelines. Contributors were mostly DPO entities and NGOs.
- Later in May, the EDPB opened public consultations on both [Guidelines 04/2022 on the calculation of administrative fines under the GDPR](#) and [Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement](#). Guidelines 04/2022 received feedback from 33 entities, whereas Guidelines 05/2022 received 14 contributions. While contributors to the former Guidelines are in majority DPO entities and business associations, Guidelines 05/2022 received feedback from a mix of contributors such as public authorities, academic institutions and NGOs.
- In late June, public consultations were opened for [Guidelines 07/2022 on certification as a tool for transfers](#). A total of 20 contributions were made, nine of which were written by business associations.
- Two guidelines were also published for consultation in October, namely: [Guidelines 8/2022 on identifying a controller or processor's](#)

lead supervisory authority and Guidelines 9/2022 on personal data breach notification under GDPR. There were six contributions to Guidelines 8/2022, and 20 contributions to Guidelines 9/2022.

- Lastly, in November, the EDPB invited feedback on [Recommendations 1/2022 on the Application for Approval](#) and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR), which were accepting contributors until 10 January 2023. Regarding these recommendations, 15 contributions were submitted.

### 5.9.3. SURVEY ON PRACTICAL APPLICATION OF ADOPTED GUIDANCE

The EDPB conducted the fifth annual survey as part of its review of activities under Art. 71(2) GDPR. The survey focused on EDPB's work and output in 2022 – particularly its guidelines, joint opinions and consultation work – to determine the usefulness of its guidance for interpreting GDPR provisions and to identify ways to better support organisations and individuals in navigating the EU data protection framework.

The survey collected the opinions of various key stakeholders with diverse interests and concerns regarding EU data protection law, in order to gather a comprehensive insight into how the EDPB's work in 2022 was perceived in the data protection and privacy sector. Among the individuals surveyed were privacy and IT experts, representatives of EU DPO organisations, as well as academics and lawyers in the field of data protection and privacy rights. The questions asked were based on a standardised questionnaire. The collected data was synthesised and common themes were identified.

In general, the surveyed stakeholders agreed that the EDPB's guidelines and joint opinions were coherent, pertinent and provided examples of practical value. Specific praises were given to the [Guidelines 9/2022 on personal data breach notification under GDPR](#), which stakeholders noted offered better examples compared to guidelines adopted in previous years. Indeed, examples were deemed clear and could be easily relied on to address real-life scenarios. With regard to [Guidelines 06/2022 on the practical implementation of amicable settlements](#), a limited number of stakeholders argued that the examples, despite being generally good, sometimes lacked clarity.

The surveyed stakeholders confirmed that they consult EDPB guidelines and joint opinions on a near-daily basis for professional purposes. It was notably indicated that the stakeholders made use of the EDPB's guidance as a basis of interpretation when dealing with different applicable laws. Most stakeholders transform the EDPB's guidelines and recommendations into practical tools to implement high-level policies. However, they also noted the challenge of swiftly doing such a transformation due to the dissimilar structure of the guidelines.

Stakeholders also pointed out that the guidelines are easily readable for experts in the field of data protection, while acknowledging that the language used is somewhat too technical for the larger public and key concepts could be made more succinct. Suggestions were made to release shorter, supplementary versions of final documents, as well as consider the adoption of infographics and hashtags of key terms to render the data more accessible. Additionally, stakeholders expressed the urgency for faster implementation of new guidelines and their revisions after public consultation.

With respect to consultations and workshops organised by the EDPB, participants expressed a desire for a more transparent overview of how their

suggestions were incorporated into the documents after the consultation process.

Regarding the accessibility of EDPB guidance on its website, stakeholders are largely satisfied. Indeed, they noted a substantial enhancement in the communication and openness of the EDPB.

In terms of the EDPB's future work, stakeholders showed their support for guidelines on the role of DPOs, as well as for updated guidance on anonymisation and pseudonymisation. Stakeholders also expressed the need for the EDPB to take a stronger standpoint when dealing with adequacy-related issues. Some stakeholders also find that guidelines covering multiple topics are harder to read than documents focusing on sector-specific issues. Thereby, they underlined the importance of adopting more sectorial guidelines in the future.

Overall, the EDPB received high praise for the quality of the guidance it provided in 2022 and was especially recognised for its success in clarifying complex GDPR concepts through the production of comprehensive documents.

The EDPB greatly values the engagement and input from stakeholders in its work and strives to implement such input in its 2023 activities. The feedback on the value of the guidance and general work of the EDPB was appreciated as it provided useful insights into the needs of stakeholders. The EDPB intends to persist in maintaining and strengthening the coherence of its efforts in the future.

### **5.10. EXTERNAL REPRESENTATION OF THE BOARD**

Public awareness and cooperation are vital to upholding data protection rights in the EEA and beyond, which is why the EDPB values stakeholder and citizen engagement. When the Chair and Deputy Chairs of the EDPB engage with other EU institutions or

bodies, or when they, or the EDPB Staff represent the EDPB at conferences and multi-stakeholder platforms, they are supported by the EDPB Secretariat. Staff from the EDPB Secretariat themselves participate in several events to promote EDPB's activities. As such, the EDPB participates in various groups and summits, such as the Global Privacy Assembly, the G7 DPA roundtable,

ENISA Advisory Group, Stakeholder Cybersecurity Certification Group.

As Chair of the EDPB, Andrea Jelinek, had more than 26 speaking engagements in 2022. These speaking engagements included press briefings, presentations and panel discussions for a range of institutes, academic forums and policy agencies. During the year, the Chair also met with European Commissioners, as well as representatives from UNESCO and the Council of the EU Working Party on Information Exchange and Data Protection, among others. Furthermore, she attended several seminars and summits on data protection and privacy matters.

In 2022, Deputy Chairs Ventsislav Karadjov and Aleid Wolfsen took part in four speaking engagements which consisted of speeches, presentations and panel discussions at several conferences and forums.

A total of 38 events were attended both physically and virtually by the EDPB Staff. These events were largely hosted by, amongst others, universities, law firms, companies and EU institutions.



# 6

## SUPERVISORY AUTHORITY ACTIVITIES IN 2022



### 6.1. CROSS-BORDER COOPERATION

Under the GDPR, national Supervisory Authorities (SAs) have a duty to cooperate to ensure the consistent application of data protection law. In cases that have a cross-border component, the SAs of the European Economic Area (EEA), i.e. the 27 EU Member States plus Iceland, Norway and Liechtenstein, have a range of tools at their disposal to facilitate harmonisation.

These tools are:

- Mutual assistance;
- Joint operations;
- The One-Stop-Shop (OSS) cooperation mechanism.

#### 6.1.1. PRELIMINARY PROCEDURE TO IDENTIFY THE LEAD AND CONCERNED SUPERVISORY AUTHORITIES

Before starting an OSS procedure for a cross-border case, it is necessary to identify the Lead Supervisory Authority (LSA) and the other Concerned Supervisory Authorities (CSAs).

The LSA is identified as the SA of the EEA country where the data controller or processor under investigation has its main establishment. To identify a controller's or processor's main establishment, one key criterion is the place of central administration. Further information on this subject is available in the [Article 29 Working Party Guidelines for identifying a controller's or processor's LSA](#), endorsed by the EDPB at its first plenary meeting on 25 May 2018.

The EDPB created workflows in the Internal Market Information System (IMI) to enable SAs to identify their respective roles. This IT platform is used to support cooperation and consistency procedures under the GDPR. The main purpose of this procedure is to define roles at an early stage.

In case of conflicting views regarding which SA should act as LSA, the EDPB acts as a dispute resolution body and issues a binding decision.

**From 1 January 2022 to 31 December 2022, there were 624 instances in which LSAs and CSAs were identified.**

#### 6.1.2. DATABASE REGARDING CASES WITH A CROSS-BORDER COMPONENT

A case with a cross-border component is registered in a central database via the IMI and may occur in several situations:

- When the data controller or processor has an establishment in more than one Member State;
- When the data processing activity substantially affects individuals in more than one Member State; and/or
- When SAs are simply exchanging information, i.e. providing each other with mutual assistance.

**Between 1 January and 31 December 2022, there were 310 entries in the database out of which 254 originated from a complaint, while 56 had other origins, such as investigations, legal obligations and/or media reports.**

Please note that:

- References to case register entries in these statistics do not have a 1-to-1 correlation to the number of cross-border complaints handled per country as multiple complaints may be bundled in one case register entry, which therefore can relate to multiple cross-border cases;
- Depending on the Member State legislation, supervisory authorities may have handled complaints outside of the Art 60 procedure in accordance with their national law.

#### 6.1.3. ONE-STOP-SHOP MECHANISM AND DECISIONS

The OSS mechanism demands cooperation between the LSA and the CSAs. The LSA leads the investigation and plays a key role in the process of reaching a consensus between the CSAs, in addition to working towards reaching a coordinated decision.

The LSA must first investigate the case while taking into account national procedural rules. During this phase, the LSA can gather information from another SA via mutual assistance or by conducting a joint investigation. The IMI also gives the LSA the opportunity to informally communicate with all CSAs to collect relevant information.

Once the LSA has completed its investigation, it prepares a draft decision, which it communicates to the CSAs. They have the right to object. This either leads to a revised draft decision or, if no consensus can be found, the EDPB acts as a dispute resolution body and issues a binding decision. The LSA must adopt its final decision on the basis of the EDPB's decision.

**Between 1 January 2022 and 31 December 2022, there were 714 OSS procedures, which resulted in 330 final decisions.<sup>2</sup>**

---

<sup>2</sup> Please note that this may include as well 'sui generis' decision in the meaning of paragraph 38 of the EDPB Guidelines 06/2022 on the practical application of Article 60(2) of Regulation (EU) 2018/1002.

The IMI offers different procedures that can be followed when handling OSS cases:

- Informal consultation procedures;
- Draft decisions or revised decisions submitted by the LSA to the CSAs; and/or
- Final OSS decisions submitted to the CSAs and the EDPB.

The OSS case register is a valuable resource to showcase how SAs work together to enforce the GDPR. It offers an exceptional opportunity to read final decisions taken by, and involving, different SAs relating to specific data subject rights.

#### **6.1.3.1. CASE DIGEST ON THE RIGHT TO OBJECT**

This section offers a case digest which analyses decisions relating to Art. 17 (right to erasure) and 21 GDPR (right to object).<sup>3</sup> The case digest was commissioned as part of the EDPB's Support Pool of Experts initiative, which aims to support cooperation among SAs by providing expertise and tools related to enforcement.<sup>4</sup>

#### **6.1.3.1.1. THE RIGHT TO OBJECT AND ITS RELATIONSHIP WITH THE RIGHT TO ERASURE IN DATA SUBJECT COMPLAINTS**

The application of Art. 21 GDPR (right to object) is often combined with the exercise of the right to erasure, as enshrined in Art. 17 GDPR. Art. 17(1) GDPR recognises this right when the data subject objects to

processing pursuant to Art. 21(1) GDPR and there are no overriding legitimate grounds for data processing,<sup>5</sup> or when the data subject objects to data processing performed for direct marketing purposes pursuant to Art. 21(2) GDPR.

Most of the cases decided by SAs under Art. 21 GDPR deal with the use of personal data for direct marketing (Art. 21(2) GDPR), rather than objections to the processing of data in the performance of tasks carried out in the public interest, in the exercise of official authority vested in the controller, or on the basis of legitimate interests (Art. 21(1) GDPR). **Thus, in the cases examined, there is a frequent link between the request to stop any further processing of personal data for marketing purposes<sup>6</sup> and the request to erase previously collected data.**

Against this background, two main sets of issues characterise the case law on Art. 21 GDPR, as emerging from the decisions adopted within the cooperation mechanism provided for in Art. 60 GDPR: (i) issues

---

tical implementation of amicable settlements.

<sup>3</sup> The analysis is based on the information gathered and the outcomes of the relevant inspection activities carried out as referred to by the SAs in their final decisions. This may entail some limitations in having a comprehensive view of individual cases.

Finally, since in the vast majority of cases the right to erasure is associated with right to object, the case law on Art. 21 GDPR is discussed before the decisions relating to Art. 17. This follows the most common sequence of requests that the SAs have to deal with and whose order contributes to shaping their decisions.

<sup>4</sup> This thematic section was produced by Alessandro Mantelero (9 December 2022), who was contracted in the framework of the Support Pool of Experts.

<sup>5</sup> See Section III.3 below.

<sup>6</sup> Art. 21(2) and Art. 21(3) GDPR.

concerning effective exercising of the right to object by data subjects, and (ii) issues relating to the procedure adopted by data controllers and processors in handling complaints from data subjects.

#### 6.1.3.1.2. EXERCISE OF THE RIGHT TO OBJECT

Three particular elements relevant to the exercise of the right to object are highlighted: (i) the information provided to the data subject about the right to object,<sup>7</sup> (ii) the solutions – including technical solutions – adopted to make the exercise of this right easier, and (iii) the implementation of appropriate procedures to handle such requests. The first two elements are discussed in this section, while the last one is covered in Section 6.1.3.3.

Several cases concern non-compliance with the GDPR because the controller did not provide data subjects with any **information on the right to object**, in contrast with Art. 13(2)(b) GDPR [EDPBI:ES:OSS:D:2021:263].<sup>8</sup> One such case decided in 2021 concerned a complainant receiving direct marketing by email from a bank without receiving information about the right to object to the processing of personal data for direct marketing purposes, pursuant to Art. 21(4) GDPR [EDPBI:NO:OSS:D:2021:292]. Data subjects were targeted with direct marketing emails without having the option to opt out when registering their email

addresses, and were only able to do so by changing their preferences once they had accessed the online banking service, or by contacting customer service.<sup>9</sup>

This case is also relevant in highlighting some recurring shortcomings in the **technical and organisational solutions** adopted by controllers in dealing with this type of request. These include lack of capacity and backlogs in customer service departments [EDPBI:NO:OSS:D:2021:292], as well as incorrect processing of objection requests [EDPBI:EE:OSS:D:2019:55], where the data subject's request was not properly registered resulting in the implementation of the objection with regard to only one account in a case of multiple user accounts and technical errors within the system [EDPBI:CZ.OSS:D:2021:312] creating delays in complying with Art. 21 GDPR.<sup>10</sup>

It is worth noting that the controller is required to facilitate the exercise of data subject rights<sup>11</sup> and that, in the context of information society services, the right to object may be exercised by automated means using technical solutions.<sup>12</sup> Although shortcomings regarding the exercise of the right to object are often part of a broader lack of compliance by data controllers, a focus on the design of the legal and technical solutions used to enable the exercising of this right plays a crucial role in terms of compliance.<sup>13</sup>

<sup>7</sup> See also, *inter alia*, CJEU, case C-201/14, *Smaranda Bara and Others v Președintele Casei Naționale de Asigurări de Sănătate, Casa Națională de Asigurări de Sănătate, Agenția Națională de Administrare Fiscală (ANAF)*, para 33.

<sup>8</sup> See Recital 70 relating to the right to object for direct marketing.

<sup>9</sup> In this case, the LSA issued a reprimand and ordered the controller to implement measures to ensure that personal data is no longer processed for direct marketing when so requested by data subjects and to ensure that data subject requests under Art. 15 to Art. 22 GDPR are answered within the time limits set in Art. 12(3) GDPR.

<sup>10</sup> See also Art. 12(3) GDPR.

<sup>11</sup> See Article 29 Working Party guidelines on transparency under Regulation (EU) 2016/679, adopted on 29 November 2017 and revised on 11 April 2018, available at <https://ec.europa.eu/newsroom/article29/items/622227/en>, accessed 10.10.2022, 26-27. These guidelines were endorsed by the EDPB on 25 May 2018.

<sup>12</sup> See Art. 21(5) GDPR.

<sup>13</sup> See e.g. EDPBI:FR:OSS:D:2019:73; EDPBI:FR:OSS:D:2019:8.

Finally, as regards how this right can be exercised, in the cases reviewed the data subjects were not asked for a request in legal terms, as even a generic request not to receive further marketing messages (such as “I ask for a guarantee that this will not repeat itself”, EDPB:NO:OSS:D:2021:292) could be considered appropriate.

### **6.1.3.1.3. COMPLAINTS HANDLING PROCEDURE**

Most of the cases decided under Art. 60 GDPR show deficiencies in the internal procedure adopted to deal with such requests,<sup>14</sup> including related aspects such as the accuracy of the procedure and internal communication,<sup>15</sup> the timeframe for processing requests,<sup>16</sup> and accountability (e.g. evidence that a system for receiving/tracking complaints has been put in place).<sup>17</sup>

Legal design elements play an important role in enabling the right to object in relation to this procedural dimension. **Cumbersome procedures** and **language barriers** should be avoided.<sup>18</sup> This should prevent cases such as the one when a contact email address was provided for the exercise of data subjects' rights, but an automated response referred the data

subject to the “Contact us” form on the website, thus setting up a cumbersome procedure instead of directly handling the requests through the contact email [EDPB:FR:OSS:D:2022:326].

**The design of interaction with the data subject** must therefore be carefully considered, using a clear and easily accessible form (see Art. 12 GDPR)<sup>19</sup> and avoiding any misunderstanding. For example, when using a no-reply email address for marketing purposes, data subjects must be informed in a clear manner and in the body of such emails that the message does not allow replies to the sender and, therefore, that any objections expressed by replying will be ineffective.<sup>20</sup> In addition, emails acknowledging receipt of objection requests must provide data subjects with timely information on the timeframe for implementation of their requests; data subjects must then be correctly informed about the outcome of the exercise of their rights.<sup>21</sup>

**Specific procedures to process objection requests – including appropriate technical solutions** – must therefore be adopted by data controllers, involving data processors according to the task distribution relating to processing operations,<sup>22</sup> being aware that

<sup>14</sup> See EDPB:DEBE:OSS:D:2021:184; EDPB:ES:OSS:D:2021:263; EDPB:NO:OSS:D:2021:292; EDPB:CZ.OSS:D:2021:312; EDPB:-FR:OSS:D:2022:326.

<sup>15</sup> See EDPB:UK:OSS:D:2019:31.

<sup>16</sup> See EDPB:DEBE:OSS:D:2018:9.

<sup>17</sup> See EDPB:CY:OSS:D:2019:57; EDPB:CY:OSS:D:2019:58; EDPB:FR:OSS:D:2020:84.

<sup>18</sup> See Art. 12 GDPR. See also Article 29 Working Party, Guidelines on transparency under Regulation (EU) 2016/679, adopted on 29 November 2017 and revised on 11 April 2018, available at <https://ec.europa.eu/newsroom/article29/items/622227/en>, accessed 10.10.2022, 10. These guidelines were endorsed by the EDPB on 25 May 2018.

<sup>19</sup> See Art. 12 GDPR. See also EDPB, Guidelines 01/2022 on data subject rights - Right of access, Version 1.0, Adopted - version for public consultation, available at [https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right\\_en](https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en), accessed 20.11.2022, 42-44.

<sup>20</sup> See e.g. EDPB:FR:OSS:D:2019:8.

<sup>21</sup> See EDPB:EE:OSS:D:2019:55 and EDPB:FR:OSS:D:2019:41.

<sup>22</sup> See e.g. EDPB:FR:OSS:D:2020:84, EDPB:MT:OSS:D:2019:60, and EDPB:EE:OSS:D:2019:55.

an incorrect task allocation may delay an appropriate response.<sup>23</sup>

In addition, the technical solutions implemented must be effective and **designed with the different types of data subject in mind**. For example, it is inappropriate to use an unsubscribe link at the bottom of direct marketing emails referring to a specific customer account page, since prospects who do not have a customer account cannot unsubscribe via this link. Here, a link that directly unsubscribes the user is much more effective than referring to the customer account.<sup>24</sup>

Although setting up specific procedures for exercising the right to object is desirable, it is worth noting that this should not limit data subjects' possibilities to send requests to the controller in other ways. However, **informal requests**, such as through a tweet on Twitter, can legitimately be disregarded by the controller when other more formal channels, such as email, are available [EDPBI:SE:OSS:D:2021:276]. Establishing specific and appropriate procedures that data subjects can use for their requests helps handle them carefully, whereas leaving room for the initiative may lead to difficulties, such as when data subjects' requests are sent using a different email address than the one used to create the personal account.<sup>25</sup>

Finally, to ensure effective regulatory compliance, **accountability** plays a crucial role in terms of record-keeping of the objection requests and their outcome.<sup>26</sup> A **data controller is responsible** for mistakes of its employees in dealing with data subjects' requests, and the employee's fault is irrelevant in assessing compliance with the GDPR and proving accountability in the cases examined [EDPBI:DEBE:OSS:D:2021:184].

### **6.1.3.2. CASE DIGEST OF THE RIGHT TO ERASURE**

#### **6.1.3.2.1. THE RIGHT TO ERASURE IN CASE LAW UNDER ART. 60 GDPR**

Despite the significant development of the right to be forgotten in the online context after the Google Spain case,<sup>27</sup> very few decisions have been adopted over the years by SAs on this topic under Art. 60 GDPR.<sup>28</sup> The large majority of the cases deal with requests for: (i) erasure as a result of objecting to the processing of data for marketing purposes [e.g., EDPBI:CZ:OSS:D:2021:312],<sup>29</sup> including unsolicited emails [e.g., EDPBI:NO:OSS:D:2022:314], and (ii) erasure of accounts/profiles relating to services no longer used.<sup>30</sup>

As the cases examined largely concern fairly basic situations, at least from the point of view of compliance with Art. 17 GDPR, the main considerations are: (i) bottlenecks and shortcomings in the internal

<sup>23</sup> See EDPBI:UK:OSS:D:2019:31 in a case where the customer care officer had forwarded the data subject's request to the wrong department.

<sup>24</sup> See e.g. EDPBI:FR:OSS:D:2020:84.

<sup>25</sup> See also EDPBI:MT:OSS:D:2019:60 and Section III.2 on the right to erasure.

<sup>26</sup> See also EDPBI:CY:OSS:D:2019:57; EDPBI:CY:OSS:D:2019:58.

<sup>27</sup> CJEU, case C 131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, available at <https://curia.europa.eu>.

<sup>28</sup> This is probably due to the fact that many of them are handled as local cases under Art. 56(2) GDPR. See the Internal EDPB Document 1/2019 on handling cases with only local impacts under Art. 56(2) GDPR, Example 11, page 10.

<sup>29</sup> See also EDPBI:DEBE:OSS:D:2018:9 and Section II.1.

<sup>30</sup> See e.g. EDPBI:DESL:OSS:D:2019:11.

complaints handling procedure, and (ii) the presence of an overriding legitimate interest or other conditions justifying the processing despite the request for erasure. In view of the large number of requests they receive, data controllers usually put in place partially or fully automated procedures to deal with them.

As for the right to erasure, complaint procedures can be divided into two main steps: the exercise of the right based on the data subject's request (see para 6.1.3.2.2.) and the complaints handling procedure (see para 6.1.3.2.3.). As a result, the issues related to these two phases are different, focusing more on the correct identification of the data subject as far as erasure requests are concerned, and more on the classification of requests and internal organisation as regards the complaint handling phase.

#### **6.1.3.2.2. EXERCISE OF THE RIGHT TO ERASURE**

As in cases relating to the right to erasure, the data controller must **facilitate the exercise of the data subject's right**<sup>31</sup> without creating cumbersome procedures. In this regard, critical issues concern the identification of the data subject and the **proof of identification**.<sup>32</sup> Although Art. 12(6) GDPR allows the data controller to ask for additional information in

event of reasonable doubt as to the identity of a data subject, a specific assessment is required to determine whether a reasonable doubt exists.<sup>33</sup>

Additional information for the purposes of Art. 12(6) GDPR should therefore be justified on a case-by-case basis. Requiring a copy of a national ID card by default is not acceptable.<sup>34</sup> The undue request of identity documents as a condition for the exercise of the right to erasure violates the principle of data minimisation pursuant to Art. 5(1)(c) GDPR. Failure to comply with such a request cannot therefore justify delaying the erasure of the data and, as the data subject's personal data could have been deleted at the time of the request, the continued processing of personal information after receipt of the erasure request constitutes an infringement of Art. 6(1) GDPR.<sup>35</sup>

A common argument used to justify the need to provide an official identity document relates to the problem raised by sending the erasure request via an **email address other than the one used at the registration stage**. Although in such cases the identity of the data subject may be uncertain on the basis of the sole email address, other solutions more in line with the minimisation principle are available. It would, for example, be disproportionate to require a copy of an identity document in the event where the data

<sup>31</sup> Art. 12(2) GDPR.

<sup>32</sup> See e.g. EDPB:DK:OSS:D:2019:69.

<sup>33</sup> See also Recital 64 GDPR and Article 29 Working Party, Guidelines on the right to "data portability" (wp242rev.01), available at <https://ec.europa.eu/newsroom/article29/items/611233/en>, accessed 10.10.2022, 13, and EDPB:FR:OSS:D:2019:3 (the online nature of the customer relationship cannot in itself imply such a reasonable doubt and be a sufficient reason to require a proof of identity; the latter must be justified by specific circumstances, such as suspicion of identity theft or account piracy). These guidelines were endorsed by the EDPB on 25 May 2018.

<sup>34</sup> See also EDPB:FR:OSS:D:2019:3 (the practice of requiring individuals to "systematically provide a copy of an identity document for exercising their rights [...] does not, in view of its systematic nature, comply with the text [of the applicable law]"') and EDPB:IE:OSS:D:2020:166 (in a case where the standard procedure of the data controller was to ask for the submission of a copy of a national identity card for all erasure requests, the LSAs had made it clear that "the request for a copy of a national identity card was not made on foot of any specific doubt as to the complainant's identity, but rather was a result of the policy that was in place in Groupon at the time") and EDPB, Guidelines 01/2022 on data subject rights - Right of access, Version 1.0, Adopted - version for public consultation, available at [https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right\\_en](https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en), accessed 20.11.2022, 23-27.

<sup>35</sup> See EDPB:IE:OSS:D:2020:166.

subject made their request within an area where they are already authenticated.<sup>36</sup> Conversely, it is possible, for example, to provide a unique identifier to users at the end of the registration process,<sup>37</sup> to inform users that only requests from an email address linked to their profile will be taken into account, to provide a password hotline in order to change the account login details,<sup>38</sup> to use other means of identification, such as via an online call,<sup>39</sup> or to identify the claimant by asking for additional information related to the service (e.g. current and previous nicknames, date of account registration, secret questions) [EDPBI:EE:OSS:D:2021:294].

In the case of robot-generated requests, the measures taken by data controllers to cope with the increased workload generated by these types of requests, cannot limit the exercise of the subject's rights by adopting **semi-automated procedures for sending erasure requests** that lead to disregarding any requests that do not follow the instructions.<sup>40</sup>

Furthermore, in the cases of Art. 17(1) GDPR, including ones in which the data subject withdraws consent (Art. 17(1)(b) GDPR) or objects to processing under Art. 17(1)(c) GDPR, a specific request of erasure from the data subject is not necessary, as there is an independent obligation arising for the data

controller to delete data regardless of the request<sup>41</sup> [EDPBI:DEBE:OSS:D:2021:229].

### 6.1.3.2.3. THE COMPLAINTS HANDLING PROCEDURE

An effective exercise of the right to erasure requires adequate management of the internal processes. This is especially true when requests are on a large scale, as in the case of erasure based on objections to data processing for marketing purposes. In this context, different types of shortcomings may occur that jeopardise the effective exercise of the data subject's right.

The main shortcomings detected by the LSAs can be classified under two categories, namely **procedural shortcomings and human errors**, where the former are more impactful in terms of GDPR compliance as they affect all requests handled, while the latter are case specific.

Among the procedural shortcomings, the most serious concerned the **complete absence of a specific procedure to deal with erasure requests**,<sup>42</sup> while the most frequent case concerns delays in the erasure

---

<sup>36</sup> See EDPBI:FR:OSS:D:2019:3.

<sup>37</sup> See EDPBI:DK:OSS:D:2019:69.

<sup>38</sup> See also EDPBI:LU:OSS:D:2019:14 and EDPBI:LU:OSS:D:2020:94.

<sup>39</sup> See also EDPBI:MT:OSS:D:2019:26.

<sup>40</sup> See EDPBI:DK:OSS:D:2020:151.

<sup>41</sup> See EDPBI:DEBE:OSS:D:2021:229 as well as the EDPB Opinion 39/2021 on whether Art. 58(2)(g) GDPR could serve as a legal basis for a supervisory authority to order ex officio the erasure of personal data, in a situation where such request was not submitted by the data subject, paragraph 22 ("Article 17 GDPR provides for both (i) an independent right for data subjects and (ii) an independent obligation for the controller. In this regard, Article 17 GDPR does not require the data subject to take any specific action, it merely outlines that the data subject "has the right to obtain" erasure and the data controller "has the obligation to erase" if one of cases set forth in Article 17(1) GDPR applies") and paragraph 23 ("some cases set forth in Article 17(1) GDPR clearly refer to scenarios that the controllers must detect as part of their obligation for erasure, independently of whether or not the data subjects are aware of these cases").

<sup>42</sup> See also e.g. EDPBI:MT:OSS:D:2019:60.

process due to poor internal organisation<sup>43</sup> or technical malfunction, which is why, for example, the data controller must adopt appropriate technical solutions not to leave an old contact email address unmonitored (e.g., automatic reply informing about the new contact email address or an automatic re-directing to the correct email) [EDPBI:MT:OSS:D:2021:212].<sup>44</sup>

The relationship between data controller and data processor, if not properly managed, may also lead to **lack of coordination/instructions in the handling of requests**, with the result that the effective exercise of the right to erasure may be impaired.<sup>45</sup>

In some limited cases, **inadequate technological solutions** are the main reason for the failure to fully meet the data subject's requests, such as when documents sent by users via email to the data controller have been stored by generating URL links making their subsequent deletion more difficult [EDPBI:FR:OSS:D:2021:202, in a case where customers' driving licenses were accessible via any browser without required authentication by entering a URL that linked to the software used for data storage].<sup>46</sup>

Finally, in several cases, the data controller complied with the data subject's request for erasure but **did not inform the data subject** of the erasure (Art.I 12(3) GDPR) [EDPBI:LU:OSS:D:2021:240]<sup>47</sup> or this information was provided with delay.<sup>48</sup>

With regard to the controller's obligation to inform the data subject about the action taken on the requests received (Art. 12(3) GDPR), the case law considered has also clarified that, when the controller notifies the data subject that the request has been granted, the erasure has been initiated and how long it will take at most, no confirmation that the erasure had been carried out is required. This is unless the data subject requests otherwise, or it is indicated that the data subject wishes to be notified that the erasure has been carried out or that the erasure is not carried out within the specified time limit [EDPBI:SE:OSS:D:2021:303].

As regards **human errors**, they may concern requests inadvertently not processed or not forwarded to the competent department [EDPBI:DEBE:OSS:D:2020:130; EDPBI:CY:OSS:D:2021:267], as well as occasional misclassification of the data subject's requests [EDPBI:DEBE:OSS:D:2021:184; EDPBI:SE:OSS:D:2021:195] or misrepresentation of the data subject's position.<sup>49</sup>

---

<sup>43</sup> See also EDPBI:DEBE:OSS:D:2018:10 in a case where the erasure request was not handled in a timely manner as there were two separate databases, managed by the customer care and the in-house shop management, and the account was deactivated on the former, but the request was not forwarded to the shop management.

<sup>44</sup> See also EDPBI:CZ:OSS:D:2021:312; EDPBI:FR:OSS:D:2020:105.

<sup>45</sup> See also e.g. EDPBI:CY:OSS:D:2021:305 in a case of an oral request for erasure, where the LSA emphasised that both the data controller and the provider must facilitate the exercise of the right of erasure by properly training their employees and, as far as the controller is concerned, adopting clear instructions on the handling of the erasure requests; and EDPBI:DEBE:OSS:D:2021:374 in a case where the data processor treated a data subject's request internally instead of forwarding it to the controller, as required by the nature of the service and task allocation.

<sup>46</sup> See also EDPBI:FR:OSS:D:2020:193 where the data subject's request for erasure was addressed by assigning personal information a special status making them unusable by the data subject, but without erasing them from the database.

<sup>47</sup> See also EDPBI:DEBE:OSS:D:2020:156, see also EDPBI:FR:OSS:D:2020:84.

<sup>48</sup> See also EDPBI:HU:OSS:D:2020:118.

<sup>49</sup> See also EDPBI:PL:OSS:D:2020:194, in a case of wrongful compliance with the data subject's request for erasure due to lack of the information on one of the several active processing operations concerning the data subject.

In addition, a combination of procedural and human errors is likely to occur in the case of erasure **requests handled manually and not via digital communications and automated procedures.**<sup>50</sup>

Based on the case law of the LSAs and in the light of the EDPB guidelines,<sup>51</sup> data controllers are required to ensure the effectiveness of all data subjects' requests concerning the exercise the right of erasure, and personal data must be systematically erased when requested.

Against this background, the automation of the complaint process can reduce both the procedural and human errors, by introducing user-friendly interfaces that support data subjects in formulating and providing better evidence of their requests, and by setting the decision-making process regarding erasure so as to be aligned with the tasks assigned under the GDPR to those handling personal data. This ensures more effective compliance with both the data subjects' requests and the GDPR, without prejudice to the human decision on each case, which remains in the hands of the persons tasked by the controller to make the final decision. In the most basic cases, such as erasure resulting from contract/service termination, full automation may be considered.

#### 6.1.3.2.4. OVERRIDING LEGITIMATE INTEREST AND OTHER CONDITIONS JUSTIFYING DATA PROCESSING DESPITE A REQUEST FOR ERASURE

More complicated issues, entailing a case-by-case assessment and the involvement of a human decision-maker, arise in cases where the request for erasure

cannot be accepted due to the presence of overriding legitimate grounds for the processing (Art. 17(1)(c) GDPR), or where the right to erasure is not granted when processing is necessary under Art. 17(3) GDPR.

As to the first category of cases, they mostly deal with the prevalence of data **controllers' legitimate interest** [e.g. [EDPBI:SE:OSS:D:2021:196](#) where the data subject's right to the erasure of banking information did not override the legitimate interest of the data controller in payment and fraud prevention, in a case involving the use of unique payment instrument identifiers to counter the abuse of free trial online services offered by a media company]. In this regard, it is worth noting that the decisions examined do not include cases of the exercise of right to be forgotten in the context of the activity of search engines, which are instead common in national and regional decisions of individual Supervisory Authorities.

Regarding the second category, i.e. cases where the right to erasure is not granted, the LSA decisions mainly concern **obligations under national laws** setting mandatory data retention periods [e.g., [EDPBI:DK:OSS:D:2021:210](#) data retention required by the law with regard to customers' complaints and purchases].<sup>52</sup> Data controllers must **inform data subjects about the legal grounds** for retaining their data, which justifies the rejection of any erasure request [[EDPBI:MT:OSS:D:2022:340](#), regarding anti-money laundering obligations; [EDPBI:MT:OSS:D:2021:272](#), concerning various obligations under banking laws]. In these cases, **specific information on the source of the legal obligations** must also be provided to the data subject at the time of the request for erasure (Article 12.1) [[EDPBI:MT:OSS:D:2021:272](#)].

<sup>50</sup> [EDPBI:SE:OSS:D:2021:178](#) in a case where the data subject was not informed about the results of the erasure request, as the request was handled manually, because it was received by mail, whereas the company used to handle requests through an automated digital system where notifications about measures taken were sent automatically.

<sup>51</sup> See Article 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, WP 253, available at <https://ec.europa.eu/newsroom/article29/items/611237/en>, accessed 10.10.2022, 12; “[...] failure to read and abide by existing policies, human error, failure to check for personal data in information published, failure to apply technical updates in a timely manner, failure to adopt policies (rather than simply failure to apply them) may be indicative of negligence”.

<sup>52</sup> See also CJEU, case C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni.

However, **legal obligations must be interpreted in line with data protection principles** and not abused to justify limitations to the rights of the data subject. In this sense, for example, the consumer's right to claim compensation for a defective product for two years after the delivery of the goods to the purchaser cannot justify a refusal to erase a customer's profile because of the use of an online form on the customer's page to exercise the right to complain, as it is possible to complain about a product in a different way with no need to maintain an active profile.<sup>53</sup>

**Legal obligations and the defence of legal claims** (Art. 17(3)(e) GDPR) related to consumer protection may also justify the retention of personal data processed in connection with orders during the time when purchasers may make their claims, or a competent supervisory body may carry out an inspection [EDPBI:CZ:OSS:D:2021:312].

Nonetheless, it is worth emphasising that, while under certain circumstances some personal data may be kept in intermediate storage in the presence of an erasure request, those that are not necessary in the context of fulfilment of such obligations or purposes under Art. 17 GDPR must be deleted after the exercise of this right [EDPBI:FR:OSS:D:2021:279; EDPBI:FR:OSS:D:2021:310].

#### 6.1.3.3. CONCLUDING REMARKS

Due to the nature of the cases decided, most of the complaints relating to Arts. 17 and 21 GDPR concern minor violations and are often characterised by a collaborative approach on the part of the data controller, with spontaneous remediation of the infringement, including the adoption of new procedures fully compliant with the GDPR.

For this reason, discontinuation of data processing and erasure of personal data as a result of LSA

investigations and active cooperation by data controllers make reprimands the main outcome in the case law examined. It is worth noting that, in presence of minor violations, the motivation of the remedy adopted in the final decision is sometimes quite brief, by using general statements (see e.g., [EDPBI:DEBE:OSS:D:2021:184](#) which refers to "the specific circumstances of the case under investigation").

Although in some cases the LSAs have imposed specific sanctions on data controllers, this is usually due to a large number of infringements of the GDPR, with a minor role played by violations of Arts. 17 and 21 GDPR. This also makes it difficult to identify in the Register a set of notable case studies focusing on these specific legal grounds.

Finally, it is worth noting that even where the violations of Art. 17 GDPR are more serious, the LSAs may consider refraining from imposing a fine in consideration of the specific circumstances of the case [e.g. [EDPBI:DEBW:OSS:D:2021:203](#) where the LSA took the following elements into account: "First of all, it must be seen that [the data controller] is a non-profit and thus not commercially active company which, apart from the managing sole shareholder, has no employees and is dependent on donations for its non-profit activities, which in 2020 amounted to only EUR 10,603.00 up to the time of the statement of 24 November 2020. In addition, did not act intentionally, but on the contrary, due to a lack of technical expertise, was convinced that the signature list had already been deleted and had thus complied with the complainant's request for erasure".

#### 6.1.4. MUTUAL ASSISTANCE

The mutual assistance procedure allows SAs to ask for information from other SAs or to request other measures for effective cooperation, such as requests

<sup>53</sup> See also [EDPBI:DK:OSS:D:2020:171](#) and [EDPBI:DK:OSS:D:2021:210](#) where it was deemed unnecessary to keep the customer account active for at least two years after the purchase for the exercise the right to complain under the customer protection law, as this right can be exercised by other means such as emails or telephone.

to carry out prior authorisations and consultations, inspections and investigations. Mutual assistance can be used for cross-border cases subject to the OSS procedure, either as part of the preliminary phase, to gather the necessary information before drafting a decision, or for national cases with a cross-border component.

The IMI enables the use of either informal mutual assistance without any legal deadline (voluntary mutual assistance) or the use of formal mutual assistance. In the latter case, according to the GDPR, the SA from which information has been requested has a legal deadline of one month to reply.

**Between 1 January 2022 and 31 December 2022, SAs initiated 248 formal mutual assistance procedures and 2924 voluntary mutual assistance procedures.**

#### 6.1.5. JOINT OPERATIONS

The GDPR allows SAs to carry out joint investigations and joint enforcement measures. Similar to the Mutual Assistance procedure, SAs can use joint operations in the context of cross-border cases subject to the OSS procedure, or for national cases with a cross-border component.

In 2022, SAs did not carry out any joint operation.

### 6.2. NATIONAL CASES

SAs have different investigative, advisory and corrective measures at their disposal to ensure entities within their countries apply data protection law correctly and consistently. Corrective measures include the following:

- Issuing warnings to a controller or processor where its intended processing operations are likely to infringe the GDPR;

- Issuing reprimands to a controller or processor where processing operations have infringed the GDPR;
- Ordering the controller or processor to comply with a data subject's request or to bring processing operations into compliance with the GDPR;
- Imposing processing limitations, bans or fines.

#### 6.2.1. SOME RELEVANT NATIONAL CASES WITH EXERCISE OF CORRECTIVE POWERS<sup>54</sup>

SAs play a key role in safeguarding individuals' data protection rights. They can do this by exercising corrective powers. The EDPB website includes a selection of SA supervisory actions. This section of the Annual Report contains a non-exhaustive list of certain national enforcement actions in different EEA countries carried out outside the OSS cooperation mechanism.

The cases examined in this section highlighted a lack of proper technical and organisational measures for processing personal data securely, which led to data breaches. Several other cases revolved around data processing without a data subject's consent. Some significant incidents also involved the unlawful processing of special categories of personal data, such as health data. Moreover, numerous cases involved data subjects who could not effectively exercise their rights, such as the right of access, the right to erasure and the right to object to data processing. Finally, a great number of cases also included the controller's failure to notify the data subjects of the occurred or the potential risk of data breaches. Entities from both the private and public sectors were fined by the national SA.

---

<sup>54</sup> This selection of enforcement actions only includes those that were sent to the EDPB by the SAs following a request to submit national enforcement news. Further cases can be found on [https://edpb.europa.eu/news/news\\_en](https://edpb.europa.eu/news/news_en).

### 6.2.1.1. BELGIUM

In 2022, the Belgian SA investigated several complaints and discovered violations by data controllers on issues related to, among others, security of processing, sensitive data, consent, transparency, cookies, thermal cameras and COVID-19.

In April, there were two cases worth highlighting. In the first one, the Belgian SA established that the controllers, Brussels Airport and Ambuce Rescue team, did not have a valid legal basis under Arts. 6(1) and 9(2) GDPR for carrying out temperature checks on passengers and for the processing of special categories of personal data (health data) in the context of the COVID-19 crisis. Moreover, one of the controllers infringed Arts. 12 to 14 GDPR due to a lack of transparency vis-à-vis the data subjects. Administrative fines of respectively EUR 200,000 and EUR 20,000 were imposed by the Litigation Chamber on the controllers. Later, the Market Court of Brussels (Court of Appeal) reduced the fine imposed by the Belgian SA on Brussels Airport to EUR 50,000 and cancelled the fine imposed on Ambuce Rescue Team.

The second case concerned the use of thermal cameras at Brussels South Charleroi Airport to check, in the context of COVID-19, whether the passengers had a body temperature of 38 degrees Celsius or above. In this regard, the Belgium Litigation Chamber held that the airport lacked a valid legal basis for processing data related to the temperature of travellers, particularly considering it processed data pertaining to a special category under the GDPR (health data). Additionally, the Belgian SA observed shortcomings in terms of purpose limitation, transparency and the information provided to travellers, as well as in the quality of the Data Protection Impact Assessment (DPIA) and the record of processing activities. As a result, the airport was issued a EUR 100,000 fine, which was later reduced by the Court of Appeal to EUR 25,000.

On 4 May 2022, a complaint was filed against the NMBS/SNCB in relation to the company's Hello Belgium Railpass, which was issued free of charge to Belgian residents during the COVID-19 crisis. It was revealed by a Twitter user that the newsletter providing information on the Railpass did not contain a possibility to unsubscribe. The Belgian SA argued that the Railpass could not be classified as a "communication from public authorities" or a "promotion at the initiative of public authorities" and as such had no legal basis under Art. 6(1)(e) and (f) GDPR. Indeed, while the controller could inform customers about COVID-related measures, it could not promote trips to tourist sites. Moreover, the newsletter did not provide an indication of the possibility to object which is a right guaranteed in Art. 21(2) GDPR. Thereby, the Litigation Chamber of the Belgian SA decided to impose a fine of EUR 10,000 on the NMBS/SNCB.

Later in May, two cases were addressed by the Belgian SA. The first case related to a complaint filed against the websites sos-services.be and sos-avocats.com. According to the plaintiff, these websites, operated by the same controller, listed lawyers and other professionals without valid legal basis and without the lawyers being informed about the processing of their personal data. Additionally, the plaintiff argued that the information was erroneous and that testimonies were falsely attributed to the listed lawyers. In addition, a lack of compliance with the GDPR of the privacy and cookie policy on the two websites was also raised. The Belgian SA imposed a fine of EUR 5,000 on the controller and ordered that the processing of personal data related to the lawyers be stopped and the data be deleted. It also ordered the controller to submit within three months a revised and compliant cookie and privacy policy to the Belgian SA's Litigation Chamber.

In the second case, a press website named the Roularta group was imposed a fine of EUR 50,000 by the

Belgian SA's Litigation Chamber for failure to meet the necessary conditions for valid consent, in the context of the processing of personal data on its websites. It was established that several cookies were placed by these websites on the user's device even before the user had given his consent and that the group had failed to comply with the obligation to provide information to users in a transparent, understandable and easily accessible form. Additionally, the consent boxes for the installation of cookies by third-party partners were pre-ticked, while consent must be the result of an active action.

As a result of a thematic inquiry into the installation of cookies by the most popular Belgian press websites, a second decision was made against another Belgian press website, "the Rossel group", on 16 June 2022. Shortcomings were found by the Belgian SA in terms of the consent required for the placement of non-essential cookies, namely: prior consent, absence of consent for audience measurement and social network cookies, lack of information to the users, further browsing as well as pre-checked consent boxes. The Rossel group was fined EUR 50,000 and ordered to bring the processing of personal data in line with the provisions of the GDPR.

In July, the disclosure by the Belgian public administration of information regarding the health status of their employee, hereby the complainant, was deemed by the Belgian SA as not compatible with the principle of data minimisation. Indeed, according to Art. 5(1)(c) GDPR only certain employees, exercising specific functions are entitled to receive this information. However, in this case, the health status of the complainant was disclosed via the minutes of the staff meeting, thereby pursuing an objective distinct from the original purpose, which was for the administration to receive and process this information in its capacity as an employer. In order to prevent similar incidents from happening again, the Litigation Chamber reprimanded the Belgian public

administration and urged it to raise awareness among its staff members.

Finally, in August, the Belgian SA dealt with a case concerning security of processing. A company that developed a digital administration platform failed to implement the necessary security measures. Indeed, it did not consider the risks that are presented by processing data, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. As a result, the controller was issued a fine of EUR 2,500.

#### **6.2.1.2. BULGARIA**

The Bulgarian SA, the Commission for Personal Data Protection (CPDP), dealt with many cases in 2022. This section covers four noteworthy decisions related to the following topics: security of processing, illegal processing and dissemination, consent, public interest and sensitive data.

In October, a notification was received by the CPDP about a violation of personal data security due to non-functioning software applications at "Bulgarian Post" EAD. As a result of a subsequent inspection, it was revealed that when carrying out its activities as a personal data controller, the "Bulgarian Post" EAD did not apply sufficient technical and organisational measures. As a result of which, unauthorised disclosure of individuals' personal data was gained to the maintained information databases. Due to the unauthorised access of data by hackers, the ability to guarantee permanent confidentiality, availability, integrity and sustainability of processing systems and services was violated, as well as the ability to promptly restore access to the personal data. A sanction in the amount of BGN 700,000 (approximately EUR 358,098) was therefore imposed by the CPDP on the "Bulgarian Post" EAD for infringing Art. 32(1)(b)(c) and (d) GDPR, as well as Art. 32(2) GDPR, in connection with Art. 5(1)(f) GDPR.

Two other cases of interest were dealt with in December 2022. The first one concerned a complaint filed against a credit institution (bank), with allegations of unlawful processing of the complainant's personal data for direct marketing purposes. The CPDP argued that the email sent to the complainant, after he had terminated his relationship with the bank, regarding an offer for a "fully digital" consumer loan was not appropriate. Indeed, the bank was unable to guarantee and prove that the processing of the complainant's personal data for marketing purposes was carried out in accordance with the GDPR, which is the obligation of the controller under Art. 24 GDPR. The bank was consequently reprimanded by the CPDP and took active steps to ensure that the status of customers who have terminated their relations with the bank, will be marked from "active to "inactive" immediately after closing an account with the company.

A complaint was also filed in December by a Member of the Bulgarian Parliament with allegations of illegal dissemination on national media of data related to his health, specifically his vaccination status in the context of COVID-19. While the complainant disputed that his vaccination status was aired without his consent, the CPDP held that the processing of his personal data was lawful. Indeed, the CPDP based its decision on the argument that the person's consent is not an element of the lawfulness of personal data processing for journalistic purposes. Furthermore, the CPDP argued that the processing was carried out for the fulfilment of freedom of expression and the right to information in a democratic community.

Lastly, an ongoing case regarding the processing of personal data of deceased individuals by political parties during the national representative elections of October 2022, was opened by the CPDP in August 2022. For the time being, the CPDP established that eight political entities processed without a legal basis and in violation of the public interest, the data of less than ten deceased persons in their respective voter

lists. It remains to be seen how the CPDP will handle these administrative violations in its final decision.

### 6.2.1.3. CYPRUS

The Cyprus SA handled several cases in 2022 involving, amongst others: a journalistic article for a politically exposed person, data breach of a school's emailing tool, data breach notification by a bank and the incorrect delivery of an application form.

The first case of interest involved a failure to comply with the principles of lawfulness, fairness and transparency, data minimisation and the principle of accuracy (Arts. 5(1)(a), (c) and (d) GDPR). The Cyprus SA issued an administrative fine of EUR 10,000 to the controller in February for having published an article containing inaccurate details about the complainant's financial status, simply to satisfy the public's curiosity. The complainant was ordered to remove the relevant article from the web pages he controlled within a week.

In March, the Cyprus SA imposed two fines, one of EUR 5,000 and the other amounting to EUR 4,000, on two separate entities. The case pertained to the unauthorised usage of a school's email tool by the president of a teacher's trade union (TU). The president sent an email to all the parents of the students, using their email addresses, for trade union purposes. In doing so, the president of the TU acted as a separate controller and therefore the TU was fined for his actions. The second fine was imposed on the school for lack of appropriate technical and organisational measures to prevent the processing of email addresses by teachers, for purposes other than schooling.

Another fine was issued by the Cyprus SA in July 2022 for the infringement of the principle of integrity and confidentiality (Art. 5(1)(f) GDPR) as well as the lack of technical and organisational measures on behalf of the controller (Arts. 24(1) and 32 GDPR). The

controller in this case was a bank that was involved in three separate data breaches and as a result, was fined EUR 17,000. In the first breach, a letter addressed to a bank's customer was sent to another company, and in the second, 11,673 electronic files belonging to bank customers were accidentally sent to the same organisation. The third incident involved sending the company one electronic file which contained notice letters the bank had sent to its customers. In total, 8,500 data subjects were affected by these incidents.

The last case concerned the same infringements as the case mentioned beforehand. Indeed, in September 2022, the Electricity Authority of Cyprus (CEA) was fined EUR 5,000 by the Cyprus SA for unlawfully disclosing personal data concerning the complainant to a third party. More specifically, an application form for installing a power line, that should have been delivered to the complainant for signature, was delivered instead to his neighbour, by a CEA employee. The application form contained personal data of the complainant and it was established that the CEA employee had untruthfully signed the form that he had personally delivered to the complainant.

#### **6.2.1.4. CZECH REPUBLIC**

In 2022, the Czech SA fined a controller CZK 70,000 (EUR 2,800) for processing personal data without legal ground. The SA stated that the controller misled data subjects freshly registered with the Trade Register by offering them entry into the private and paid "Registry of Commerce and Trade", which they were ultimately prompted to pay for. As a result thereof, the controller processed the name, surname, business address, and company identification number of data subjects retrieved from the Trade Register. Although the controller processed the data which was publicly accessible in the Trade Register, the Czech SA ruled that it was not permissible to process such data freely without any legal basis.

#### **6.2.1.5. DENMARK**

In most EEA jurisdictions, SAs have the power to issue administrative fines themselves. In Denmark, however, this is not the case. Indeed, data protection law infringements are first looked into by the Danish SA before being reported to the police. After the police has conducted an investigation to determine whether charges should be filed, the court then decides on any possible fines.

In January, the Danish SA expressed serious criticism against controller Den Blå Avis for the processing of personal data of individuals visiting its website. Particularly, it was established that the controller's consent mechanism on its website did not meet the legal criteria for a valid consent. Moreover, the processing, which was conducted for analytical and statistical purposes, did not respect the core principles of the GDPR such as lawfulness, fairness and transparency.

In March, the Danish Municipality was reprimanded for revealing by email confidential health information about one of its employees. Indeed, the complainant's colleagues were notified by the municipality that the woman could no longer conduct challenging physical tasks, due to her ongoing fertility treatment. In its decision to reprimand the municipality, the Danish SA emphasized a great deal on the sensitive nature of the data which had been shared with the group of people.

In April, the Danish Financial Supervisory Authority was seriously reprimanded by the Danish SA for violating the requirement of adequate security when processing data (Art. 32(1) GDPR). The controller mistakenly supplied information regarding whistleblowers to a journalist in connection with a request for document access. Indeed, the personal data contained in the file was not successfully erased by the controller, rendering it possible for the journalist to access it. In this case, the Danish SA emphasised that in situations where the data originates from a system of whistle-

blowers, the risk of violating the rights of data subjects is greater.

In May, the Danish SA issued a decision in regard to a case concerning the use of an AI-profiling tool “Asta” by municipal authorities. The tool was used by the authorities to determine the length of the contact process between a newly unemployed person and the unemployment centre. However, this was estimated by processing data from unemployed persons and comparing it to the value of created (generic) individuals. The Danish SA came to the conclusion that an unemployed individual’s consent does not constitute a legal basis for the processing of his personal data. It particularly highlighted that in the context at hand, consent cannot be considered to have been given freely.

In June, a request was made by a data subject for access to documents related to a pending court case. However, the complainant did not specify which documents were to be reviewed by the controller to identify personal data related to him. In its final decision, the Danish SA argued that this request did not entail an obligation for the controller to search for and review the documents in order to identify and provide information about the data subject.

In October, an issue related to consent was brought to the attention of the Danish SA. The case concerned the processing of personal data of visitors to a Danish website. In its decision, the Danish SA considered that the controller of the website, JP/Politiken, failed to provide information to the visitors about the purposes of data processing. Hence, it could not be agreed that the visitors had given informed consent. Additionally, the Danish SA argued that the “accept all” option of the consent mechanism set in place by the controller conflicted with the principle of lawfulness, fairness and transparency. As a result, the Danish SA reprimanded JP/Politiken.

Several cases related to the processing of personal data of alleged victims and individuals accused of

sexual harassment were dealt with by the Danish SA in February, September and November 2022. Regarding the lawfulness of processing, the Danish SA found that a general legitimate interest exists when investigating instances of sexual harassment. It thereby argued that the controllers could process the data based on several provisions of the GDPR, namely Art. 6(1)(f), Art. 6(1)(e) or Art. 9(2)(f). However, due to a lack of information provided to the data subjects regarding the processing of their personal data, the Danish SA issued reprimands to the controllers.

#### **6.2.1.6. ESTONIA**

Upon conducting, on its own initiative, a monitoring operation of the Facebook groups that publish personal data of individuals in debt, the Estonian SA issued a decision in January 2022 against the controller. The controller, who held the position of administrator of the Facebook groups, stated that the processing was done for personal purposes. However, the Estonian SA argued this not to be true, since the groups were composed of a number of members between 4600 and 14,800, thereby entailing that the data was disclosed to an unidentified group of individuals. Ultimately, the Estonian SA recalled that the processing of information related to the financial status of individuals would infringe on their rights. The controller was issued a fine of EUR 5,000 and was requested to stop sharing individuals’ personal data in Facebook groups without their explicit consent.

The same month, the Estonian SA issued a precept with a penalty payment of EUR 10,000 on the controller Krediidiregister OÜ for each unfulfilled obligation. It requested the controller, amongst other obligations, to terminate the disclosure of all valid and invalid data of natural persons related to a legal identity. Moreover, the controller was ordered to verify that third parties who received the data had a legitimate interest.

On 25 July 2022, the Estonian SA ordered the controller Ticketer OÜ to (i) align its privacy notice

with the requirements set in the GDPR and (ii) either remove the website's third-party cookies or obtain consent from the data subjects before placing the cookies. The decision of the Estonian SA resulted from a self-initiated monitoring operation to assess the way personal data is processed in various ticket seller portals. During the operation, it was revealed that the controller's website lacked a privacy notice as well as other GDPR requirements, such as a purpose and a legal basis for processing. The Estonian SA issued a precept with a penalty payment of EUR 5,000 for each unfulfilled point.

#### **6.2.1.7. FINLAND**

In this section, seven cases from the Finnish SA's work related to data protection violations will be presented.

On the basis of non-compliance with an order issued by the Finnish SA, a telemarketing company was awarded an administrative fine of EUR 8,300 on 29 April 2022. The Finish SA decided that the controller had failed to comply with its order to fulfil a customer's request to access the recording of a sales call. Having access to the recording would have enabled the customer to identify whether the telemarketing company's methods for promoting and selling its goods to older customers had been legal.

In response to the eleven cases brought to the SA concerning Otavamedia Oy, the Finnish SA adopted a decision against the controller in May 2022. Complainants criticised the controller for ignoring their requests concerning data protection rights. However, the controller shed light on a technical issue that prevented the data protection requests from being directed to customer service. Nevertheless, the Finish SA noted the controller's responsibility to ensure the functionality of the email inbox, especially as it was the main contact channel for data protection matters. Furthermore, the SA found that Otavamedia Oy had gathered a considerable amount of identification data (i.e. complainants' signatures) by imposing the

use of a printable form for data protection requests. Consequently, the controller was ordered to update its processes to comply with the requirements for data protection and was issued a fine of EUR 85,000.

On 8 June 2022, the Finish SA ordered three insurance companies to correct their activities related to the processing of health information of insurance applicants. This was ordered to ensure that future processing activities would comply with the GDPR. One of the insurance companies was notably reprimanded by the SA as it requested consent for processing health data without properly identifying the purposes behind the use of this data. Furthermore, it was revealed that the insurance companies were not clear as to whether they only limited their data requests to health information deemed necessary for assessing the liability of the company.

Later in July, the Finnish SA issued a reprimand to a bank for its failure to enable their customers' inquiry into the erasure of their personal data. The Ombudsman strongly believed that such data should have been erased and if not, the reasons for keeping it should have been communicated to the customers. The Finish SA also reprimanded the controller for erasing one of the complainant's data before the customer had been able to access it. It emphasised that in cases where a data subject wants to both access and delete personal data, then the request to access it should be completed first.

In October, the Legal Register Centre was warned by the Finish SA that its planned processing of personal data would likely infringe the GDPR. The Finish SA based its decision on the fact that the controller was unable to reduce the risks inherent to the planned processing measures. This included a risk that the data would be transferred to non-EU countries' authorities, as a result of their right of access to information.

In November, the Finish SA issued a reprimand against the Tax Administration for the failure to fully consider

the risks involved in processing personal data. Indeed, between 2015 and 2021 the controller issued requests for information regarding all cross-border credit transfers, which included data on banks' customer registers. However, the controller only limited the transactions to be investigated after having the data in its possession, and as a result, infringed the GDPR.

After having received three complaints from private individuals, the Finnish SA opened an investigation into the controller Alektum Oy. It was revealed that the controller had not only failed to give a reply to the individuals' requests to access their personal data, but also purposely delayed the investigation by avoiding the Finnish SA. In addition to being reprimanded by the SA in December 2022, the controller received a fine of EUR 750,000 for seriously violating data protection rules.

#### **6.2.1.8. FRANCE**

In 2022, France handled several cases where it issued considerably large fines. This section will present a selection of those cases.

A significant fine was first issued to a controller in April 2022. The fine amounted to EUR 1,500,000 and was served to Dedalus Biologie by the French SA regarding a massive data breach of the personal data of 500,000 people. In this case, sensitive information about the individuals' health as well as their name, social security number, name of prescribing doctor and date of examination, was released on the internet. The French SA held that the compromised data was a direct consequence of the controller's lack of satisfactory security measures.

On 23 June, TotalEnergies Électricité et Gaz France was issued a sanction of EUR 1,000,000. The French SA accused the controller of rendering it impossible for individuals to refuse commercial prospecting. When filling out a web form for subscribing to an emerging contract, the user had no means to refuse the re-use of their personal data for ulterior purposes, such as

commercial canvassing. In doing so, the controller infringed several provisions of the GDPR, notably the obligation to inform solicited individuals, the right of access to data and the right to object of data subjects, as well as the obligations relating to the modalities for exercising rights.

On 19 October, the controller Clearview AI was subjected to a maximum financial penalty of EUR 20,000,000. French SA issued the fine as a consequence of the controller's failure to comply with the SA's earlier formal notice. The formal notice ordered the controller to stop the collection and use of the data of French citizens without a legal basis and to comply with their requests for erasure. In light of the serious violations of the data subjects' fundamental rights, the restricted committee added to the fine a penalty of EUR 100,000 per day for delay in complying with the order.

In November, three interesting cases were handled by the French SA. On 10 November, the controller Discord Inc was issued a hefty fine of EUR 800,000 for having infringed several provisions of the GDPR. This included a failure to define and respect a data retention period appropriate to the purpose of processing data (Art. 5(1)(e) GDPR), to comply with the requirement of providing information to the data subjects (Art. 13 GDPR), to ensure data protection by default (Art. 25(2) GDPR), ensure personal data security (Art. 32 GDPR) as well as a failure to perform a DPIA (Art. 35 GDPR).

Later in the month, the main electric utility in France "EDF" was held accountable for omitting to consider the data rights of its customers. Indeed, the controller did not collect the consent of individuals to receive commercial emails, nor did it inform the customers about its data processing activities. Lastly, the French SA argued that EDF had failed to ensure the security of the personal data of the customers. For the reasons mentioned above, EDF was issued a fine of EUR 600,000.

Finally, the third case handled in November by the French SA concerned the challenges faced by individuals in having their requests for accessing or erasing their personal data considered by the controller Free. In addition to preventing individuals from exercising their rights to have access to their data or have it erased, the French phone operator Free failed to ensure the security of the data. The French SA established that the controller did not fulfil its obligation to document a personal data breach under Art. 33 GDPR. Free was therefore issued a fine of EUR 300,000 and ordered to comply with the requests of its customers within three months.

## 6.2.1.9. GERMANY

There are both national (federal) and regional SAs in Germany.

A case was handled by the SA of the Free Hanseatic City of Bremen in March 2022, regarding the processing by a large company of over 9,500 data. This data belonged to numerous prospective tenants and was processed by the controller without a legal basis. Moreover, the information processed constituted sensitive data specifically protected under the GDPR, such as skin colour, ethnic origin and religious affiliation. Additionally, it was discovered that the company had deliberately refused requests for transparency regarding its data processing activities. Considering the serious infringement of several provisions of the GDPR, the controller was issued three administrative fines of EUR 1,435,750, EUR 400,000 and EUR 75,000 respectively.

The same month, a second case related to the processing of personal data revealing political opinions was dealt with by the SA of the Free Hanseatic City of Bremen. In this case, a small regional political party went against the warning originally issued by the SA and proceeded to run a web-portal enabling students and parents to complain about the political views of teachers. As a consequence of having ignored the SA's

warning and subsequently infringing the GDPR, the controller was issued a fine of EUR 6,000.

In August 2022, Berlin SA issued a fine of EUR 525,000 on a subsidiary of a Berlin-based e-commerce company. The SA concluded that the controller did not honour the reprimand issued against the company in 2021. Indeed, an inspection conducted by the Berlin SA in 2022 revealed that the controller had still not fulfilled its task to monitor the compliance of his service companies with data protection regulations.

## 6.2.1.10. GREECE

In a national case before the Hellenic SA, two mobile telecommunications companies were fined in January 2022 for personal data breaches. As a result of having provided unclear and insufficient information to its subscribers, the controller Cosmote was fined EUR 6,000,000 for infringing the principles of legality and transparency. Additionally, the Hellenic SA established that the company had taken inadequate security measures and, amongst other things, conducted a poor DPIA. The other controller, Ote, was also found guilty of infringing data security principles and received a fine of EUR 3,250,000.

In another case, the Hellenic SA issued a EUR 2,000 fine to a controller for the violation of individuals' rights to object, as well as the infringement of the GDPR principles of lawfulness, fairness and transparency. This fine was issued in March 2022 after a complaint was made by a teacher that their employer regularly monitored online courses taught via "Zoom", despite the employee's objections. Furthermore, the employer failed to provide a valid legal basis for the processing in question.

On 19 July 2022, the Hellenic SA dealt with a case of unlawful processing of data revealing the balance of a debtor's debt. The processing was conducted by a loans and credits claims management company even though a judicial exemption from the complainant's

debts existed. Furthermore, by claiming that the complainant could not be identified, the controller impeded the exercise of their rights. Hence, the Hellenic SA decided to impose two fines of EUR 10,000 each on the controller for the various GDPR infringements.

A second decision was adopted by the Hellenic SA in July 2022. This decision was issued against Clearview AI Inc, a company marketing facial recognition services, for violating the principles of lawfulness and transparency. The company received a EUR 20,000,000 fine and was ordered to satisfy the complainant's request for access to personal data. Additionally, the Hellenic SA commanded the controller to delete all personal data of the Greek data subjects which it had processed using facial recognition technology. A general prohibition to process personal data using such methods was also imposed on the company.

In August, several controllers were issued fines in a case involving the publishing and processing of the results of self-tests on the electronic application "self-testing.gov.gr". Indika S.A. was fined EUR 5,000 for the lack of effective security measures, while the controller, Greek Seamen's Fund (NAT), was ordered to remove the application from its IT system as well as delete the data of ship crew members. Moreover, Indika S.A. and the Ministry of Labour and Social Affairs were reprimanded for drafting an incomplete and overdue impact assessment. Finally, a fine of EUR 5,000 was issued to both the Ministry of Interior and NAT for omitting to comply with the requirement to carry out an impact assessment.

#### **6.2.1.11. HUNGARY**

In 2022, the Hungarian SA imposed multiple fines for violations of data protection law. Selected cases are listed here:

- In February, the controller Budapest Bank Zrt was fined EUR 650,000 for processing, with the

help of software using AI, the emotional state of its clients during calls. The Hungarian SA concluded that both the legitimate interest and impact assessments failed to provide any actual risk mitigation and that data processing using AI may pose a high risk to individuals' fundamental rights.

- In April, the Hungarian SA held that the Hungarian Two Tailed Dog Party, a political satirical joke party, had not applied sufficient security measures when storing the data of sympathisers and activists. Indeed, this special data was stored online on Google sheets, thereby rendering it possible for anyone with a link to access and download it on a local computer. A fine of EUR 7,500 was issued to the Party.
- In March, a serious case regarding the publication of pornographic photographs of a data subject on a website was handled by the Hungarian SA. Even though the complainant had given consent to be photographed 10 years ago, the SA argued that such consent was not a valid legal ground for the processing activities of the website's controller, especially since the pictures featured the complainant's full legal name. Not only was the processing held unlawful, but the controller also infringed the rights of the complainant by denying its request to have the data deleted. The SA thereby ordered the controller to erase the pictures and the subject's legal name from the website.
- In August, the Hungarian SA dealt with a national case involving the processing of personal data by a financial institution during credit assessments. In the case at hand, the complainant had not given their consent to have his personal data processed during such assessments. The controller was imposed a fine of approximately EUR 78,945 for failing to refer its processing activities to an appropriate legal basis and to

- carry out an interest assessment. Moreover, adequate information had not been provided to the complainant regarding the processing and storage of their personal data.
- In October, the Hungarian SA recalled that data processing through a camera surveillance system during opening hours is unlawful, based on Section 38 of EDPB's Guidelines 3/2019. The SA held that the controller of the surveillance system not only processed the data without a valid legal basis, but also failed to adequately inform individuals of the processing activities.
  - In July, a physician was fined EUR 1,500 by the Hungarian SA for failing to be transparent regarding its data processing undertakings. The SA established that a client of the physician was refused access to a copy of the documentation laying down the care provided to her during the medical consultation. Additionally, it was discovered that the physician failed his legal duty to upload the findings electronically and provided the patients with a privacy statement containing untrue information.
  - In September, the Hungarian SA issued an administrative fine of EUR 75,000 to the controller Magyar Éremkibocsátó Kft. The controller was criticised for processing the personal data of its clients, despite having not received their informed consent. Indeed, when purchasing collectors' coins issued by the company, clients would have to check a box containing both the statement of purchase and the statement of consent to future marketing offers. The controller was therefore ordered by the SA to provide clear information to its customers.
  - Later in the month of September, TV2 Média Csoport Zrt which operates two media websites was fined EUR 25,000 by the Hungarian SA. The fine was issued as a result of the controller's failure to solve the limitations of its cookie consent management systems (CMS). Indeed, the Hungarian SA held that the CMS did not comply with the GDPR.
  - Lastly, an important case worth highlighting is the case related to the alleged use by the Hungarian law enforcement agencies and National Security Services of the spyware called "Pegasus" against investigative journalists and lawyers. On 9 August 2021, the Hungarian SA launched an investigation *ex officio* to assess whether the activities of the latter were compliant with data protection regulations. This investigation was launched after a list containing some 50,000 phone numbers, that had potentially been targeted by the surveillance tool, was leaked. In its decision, the Hungarian SA held that the processing of data with the surveillance tool Pegasus was in accordance with the relevant legal data protection regulations.
- #### **6.2.1.12. ICELAND**
- The Icelandic SA handled several cases in 2022, focusing mainly on the unlawful processing of personal data.
- On 8 March, the Harpa Concert Hall and Conference Centre was ordered to stop processing the data present on the tickets purchased by individuals for events organised by the company, such as ID numbers and dates of birth. The Icelandic SA held that this processing was not necessary as the contract of the purchase could have been fulfilled without this data. As a result of having violated the principles of legality, fairness, transparency and minimisation of data, the company was fined ISK 1,000,000 (approximately EUR 7,200) and was further instructed to delete all the collected data.
- On 3 May, the Icelandic SA issued a fine of ISK 1,500,000 (approximately EUR 10,700) on the controller HEI ehf, a medical travel agency in Iceland. The SA determined

that the controller had not established the lawfulness of the processing by its employee of several doctors' email addresses. Additionally, the complainant's right to access his personal data was infringed by the controller who deliberately erased the data before processing the request.

On the same day, 3 May, the Icelandic SA imposed a fine of ISK 5,000,000 (approximately EUR 35,768) on the municipality of Reykjavík for breaching several GDPR provisions by using Seesaw. It was established in a prior decision of the SA in December 2021, that the municipality was unlawfully processing the personal data of students using an American cloud-based service, Seesaw. The fine issued by the SA in 2022 was based on reasons stated in its first decision as well as the fact that the infringement concerned the processing of sensitive data (of children). Moreover, when calculating the fine, the Icelandic SA considered that the municipality had co-operated, that there was no indication that the violation had caused damage and that Seesaw's general information security seemed to be adequate.

#### **6.2.1.13. IRELAND**

As a result of a personal data breach involving the accidental publication of individuals' personal data on the internet, the Irish SA issued a reprimand and a fine of EUR 5,000 to Slane Credit Union Limited in January 2022. It was deemed that the controller had infringed the principle of security of processing laid down in Art. 5(1)(f) GDPR.

On 14 March, in a national case concerning the unauthorised disclosure and accidental alterations of customer personal data, the Bank of Ireland Group, a data controller, was issued a fine of EUR 463,000. Indeed, not only did the controller report the data breaches with undue delay, but it also provided insufficient information regarding the data breaches to the Irish SA. Additionally, the Irish SA established that the controller had failed to inform individuals in

a timely manner that the breaches could potentially impact their fundamental rights and freedoms. Lastly, it was discovered that when transferring the data to the Central Credit Register, the bank had not ensured a level of security appropriate to the risks involved.

On 3 May, the Irish SA, of its own volition, conducted a monitoring exercise during which it evaluated whether public sector organisations were in compliance with the requirement to designate a data protection officer (DPO). It was established in this case, that the controller Pre-Hospital Emergency Care Council failed to designate a DPO and to publish and communicate the latter's contact details to the Irish SA. Consequently, the controller was issued a reprimand.

Furthermore, three important decisions were issued by the Irish SA in December 2022.

The Irish SA imposed a reprimand on the controller An Garda Síochána as it failed to implement appropriate technical and organisational measures when processing the personal data of 108 data subjects, some of whom were children. Moreover, the controller was ordered to bring its processing activities into compliance.

In a second case concerning the unauthorised access of a large amount of personal data, the Irish SA imposed a EUR 15,000 fine on the A&G Couriers Limited T/A Fastway Couriers Ireland. This sanction was issued in light of the controller's failure to provide a level of security suitable to the risks posed by its processing of personal data.

Lastly, the third decision issued in December by the Irish SA was made in relation to the illegal access by an unknown actor, most likely through a phishing attack, of personal data of residents of the Virtue Integrated Elder Care (VIEC). The Irish SA fined VIEC, as a controller, EUR 100,000 for failing to adopt appropriate technical and organisational measures which would have protected the data of its residents

and limited the risk of access to its email system where the data was processed.

#### **6.2.1.14. LATVIA**

On 21 April 2022, the Latvian SA, known as the Data State Inspectorate of Latvia, imposed an administrative fine of EUR 1,464.13 on the controller SIA “Your Move” for the infringement of Art. 83(5)(e) GDPR. The Latvian SA found that SIA “Your Move” had failed to comply with its order to provide information about the company’s processing activities. In short, the SA ordered the company to provide an explanation regarding the personal data breach incident that took place on its website, however, the controller did not show an interest in providing the requested information. Hence, the controller failed to carry out its tasks under Art. 58(1)(e) GDPR.

#### **6.2.1.15. LITHUANIA**

The Lithuanian SA issued multiple fines in 2022. The Lithuanian SA carried out the following enforcement acts:

- Issued a fine of EUR 20,000 on a company providing credit assessment services for the processing of data on financial obligations, in breach of Art. 6(1) GDPR as well as Art. 5(1)(a) and (b) GDPR.
- Imposed a fine of EUR 6,000 on a company managing sports clubs for the failure to obtain the valid consent of its customers to process their biometric data. It was revealed that no alternatives for accessing the sports clubs other than identification through biometric data could be used by customers. In essence, the controller was fined for infringing numerous GDPR provisions, namely: principles of transparency and lawfulness (Art. 5(1)(a) GDPR), processing of special categories of personal data (Art. 9 GDPR), the right to be informed about the processing

of personal data (Art. 13(1) and (2) GDPR), processing of activity records (Art. 30(1) and (3) GDPR) and Data Protection Impact Assessment (Art. 35(1) and (3)(b) GDPR).

- Issued a fine of EUR 35,000 on an IT company for its failure to ensure the ongoing confidentiality, integrity, availability and resilience of its data processing systems and services under Art. 32(1) (b) GDPR.
- Found an applicant’s complaint concerning the disclosure of his residential address to be well-grounded. Indeed, the Lithuanian SA concluded that the controller, a public authority, had violated the principles of purpose limitation and data minimisation laid down in Art. 5(1)(b) and (c) GDPR by publishing the claimant’s personal data.
- Decided that a controller’s refusal to provide a client with a copy of the requested records of telephone conversations (which took place between the client and an employee) violated Art. 15(3) GDPR.
- Took corrective actions against a public organisation for infringing Arts. 5(1)(a), 6 and 7 GDPR. In this case, the Lithuania SA held that the controller had violated the GDPR by : (i) processing children’s image data without their consent, (ii) failing to create the possibility of free choice and the inability to withdraw consent without suffering damage, and (iii) failing to give separate consent for individual operations of persona data processing.
- Recognised an applicant’s complaint against a legal entity in the private sector as well-founded. The Lithuanian SA argued that the use by the controller of the complainant’s personal correspondence with another employee, as a ground for dismissal, violated Art. 6(1) GDPR. No grounds could be used by the controller to justify that the processing was done in a lawful manner.

- Concluded that a controller infringed Arts. 5(1) (a) and 7(2) GDPR, as well as Art. 69(1) of the Law on Electronic Communications of the Republic of Lithuania by failing to acquire the applicant's legally compliant consent to receive direct marketing messages.

#### **6.2.1.16. LUXEMBOURG**

In March 2022, the Luxembourgish SA dealt with a complaint where a data controller did not fulfil its obligation to put in place appropriate security measures when processing personal data. The Luxembourgish SA solved this issue by reprimanding the controller and ordering him to comply with the provisions of the GDPR.

A month after, a data controller was found in violation of Arts. 13, 15 and 31 GDPR and was issued a fine amounting to EUR 1,500. Particularly worth mentioning is the controller's failure to respect the right of access of the complainant, by omitting to provide him adequate information as laid down in Art. 15 GDPR and its lack of cooperation with the SA.

Two cases involving the use of video surveillance for data processing purposes were dealt with by the Luxembourgish SA in 2022.

The first case concerned the use of video surveillance and geo-tracking systems to collect personal data, which was handled by the SA in February 2022. The data controller in this case was issued a fine of EUR 4,900. The Luxembourgish SA considered that the controller did not provide data subjects sufficient information regarding the processing of their personal data (Art. 13 GDPR) and that the ranges of cameras used were disproportionate to the objective pursued (Art. 5(1)(c) GDPR). Indeed, it was found that the controller had kept the personal data collected through the geo-tracking system for longer than necessary for the purposes for which it was processed.

The second case also touched upon the topic of data processing via a video surveillance system. The use of a total of twelve cameras by the controller was deemed disproportionate and in violation of Art. 5(1) (c) GDPR. Indeed, these cameras were aimed at the public road and neighbouring buildings, meaning that employees were constantly being monitored by the controller during both their worktime and break time. The controller was therefore issued a EUR 10,000 fine.

Finally in December, the Luxembourgish SA imposed a EUR 2,100 fine on a data controller for the failure to sufficiently inform data subjects (Art. 13 GDPR) and be transparent about its data processing activities (Art. 12(1) GDPR). According to the case facts, the controller collected personal data on its internet page as well as its mobile application.

#### **6.2.1.17. THE NETHERLANDS**

In 2022, the Dutch SA imposed multiple fines for GDPR violations. Three selected cases will be analysed in this section.

The first case concerns complaints made to the Dutch SA as to how the controller Sanoma Media Netherlands B.V. handled requests from individuals to access their data and have it deleted. Customers wishing to have their requests approved were asked by the controller to first provide a copy of their identity document, something which the SA deemed to be completely unnecessary. While DPG Media, the company that took over Sanoma, later changed its practice to ensure that the data subjects' rights would no longer be impeded, the Dutch SA however, still decided to impose a sanction. A fine of EUR 525,000 was issued to DPG Media.

The second case handled by the Dutch SA in 2022, involved the processing by the Ministry of Foreign Affairs of an average of 530,000 visa applications per year in the last three years. The main concern of the SA was the failure of the Ministry to sufficiently secure

the digital system it was using (NVIS) to process the data of visa applicants. Thereby, alongside a fine of EUR 565,000, the controller was ordered to adopt appropriate security measures in line with Art. 32(1) GDPR and provide applicants with adequate information about their data processed in the context of the Schengen visa process.

Lastly, in a third case concerning the use of a blacklist to register indications of fraud, the Dutch SA imposed a hefty fine of EUR 3,700,000 on the Tax Administration for illegally processing personal data for several years in its ‘fraud identification facility’. The SA held that the use of the said blacklist by the Tax Administration greatly impacted the rights of individuals that were wrongfully added to it. Indeed, once included in this list, the individuals were registered as possible tax frauds.

#### **6.2.1.18. NORWAY**

The Norwegian SA carried out the following actions in 2022:

- Banned the processing of personal data of internet users by the controller Shinigami Eyes for failing to provide a legal basis for its processing activities. According to the SA, the controller which is a browser extension available for Chrome and Firefox, would tag individuals without their knowledge and in doing so would also give indications to other users as to whether the tagged individual was pro- or anti-trans. This subjective assessment was deemed by the SA to be a threat to the free exchange of ideas online.
- Issued a fine of EUR 5,000 on the controller Etterforsker1 Gruppen AS for performing an unwarranted credit rating on a private individual without any type of customer relationship between them.
- Imposed a hefty fine of EUR 500,000 on the Norwegian Labour and Welfare Administration

for publishing CVs of users on the service arbeidsplassen.no without the proper legal basis to do so (Art. 6 GDPR). However, it is worth mentioning that the controller took active steps to remedy the situation when the infringement was discovered.

- Ordered the municipality of Østre Toten to implement a suitable control system for information security and personal data protection, but also imposed a fine of EUR 400,000 for the failure to protect its IT systems against a serious cyberattack. This attack was made possible due to the severe and fundamental security flaws present in its systems.
- Issued the controller Storting a fine of EUR 200,000 for inadequate security. Indeed, the Norwegian SA concluded that Storting had failed to prevent the unauthorised logins to important email accounts, such as those of parliamentary representatives, by not having implemented suitable technical and organisational measures as required under Art. 32 GDPR.
- Imposed a fine of EUR 500,000 to the controller Trumf for failing to secure the processing of its members’ purchasing history. The SA held that the controller had not implemented a measure verifying whether a user registering a bank account was that account’s real owner. Members of Trumf were therefore able to easily access the purchasing history of another individual by registering with the unknown person’s account number.

#### **6.2.1.19. POLAND**

This section will highlight six cases of interest, handled by the Polish SA in 2022.

On 9 January, in a case involving the copy by unauthorized persons of an additional customer database of the controller, the Polish SA issued fines on both the controller and the processor. The controller,

Fortum Marketing and Sales Polska S.A, was issued a fine of EUR 1,080,000 for having infringed Arts. 5(1)(f), 24(1), 25(1), 28(1), 32(1) and (2) GDPR. The processor, however, was imposed a smaller fine of EUR 55,000 for violating Arts. 32(1) and (2) in relation to Arts. 28(3)(c) and (f) GDPR.

On 31 May 2022, the Polish SA issued an administrative fine of approximately EUR 2,200 on the Warsaw Centre for Intoxicated Persons for infringing, through its surveillance system, Art. 6(1) (lawfulness of processing) and Art. 5(1)(a) (principles of lawfulness, fairness and transparency) GDPR.

On 7 September, the Cultural Centre of Sułkowice municipality received an administrative fine of PLN 2,500 (approximately EUR 529) for outsourcing parts of its activities to a processor without a written contract, as required under Art. 28(3) and (9) GDPR. Furthermore, the controller failed to check that the processor had provided sufficient guarantees for the implementation of appropriate technical and organisational safeguards (Art. 28(1) GDPR).

On 2 November, the Mayor of the Commune was sanctioned for having infringed several provisions of the GDPR, namely: Arts. 25(1), 24(1), 5(1)(f) and (2), as well as 32(1) and (2). A fine of PLN 8,000 (approximately EUR 1,695) was issued by the Polish SA to the Mayor after it was revealed that he had failed to implement security measures on its portable computer device. The computer, which was stolen as a result of a break-in in the controller's apartment, contained a file with personal data of the complainants.

On 16 November, the Polish SA issued a fine of EUR 340,717.27 to a controller based in Warsaw, for infringing Arts. 5(1)(f), 5(2), 25(1), 32(1) and (2) GDPR. This sanction was imposed in light of a data breach, which took place as a result of the exploitation of the controller's vulnerable IT system. Indeed, the SA held that the controller had infringed the principle of confidentiality as it did not put in place adequate

safeguards, which would ensure that the data stored in its system is protected against unauthorised access.

Later in November, the Polish SA held that the processing of special categories of personal data of potential customers, as done by the controller Pionier, infringed Arts. 6(1), 5(1)(a) as well as 9(1) and (2) GDPR. Therefore, the controller was issued a fine of more than PLN 45,000 (approximately EUR 9,537) and ordered to cease processing the sensitive data without a legal basis.

#### 6.2.1.20. PORTUGAL

On 11 February, the Portuguese SA concluded that the Portuguese National Statistics Institute had committed, in the context of processing data obtained from its national census survey, the following five GDPR violations:

- lack of lawfulness for the processing of special categories of personal data (Art. 9(1) GDPR);
- lack of compliance with transparency obligations (Arts. 12 and 13 GDPR);
- lack of a DPIA (Arts. 35(1), (2) and (3)(b) GDPR), including all the processing activities and relevant dimensions of Census;
- lack of due diligence concerning the choice of the processor (Arts. 28(1), (6) and (7) GDPR); and
- lack of compliance with the legal requirements for international data transfers (Arts. 44 and 46(2) GDPR), as interpreted by the Court of Justice of the European Union in the *Schrems II* ruling.

A single fine of EUR 4,300,000 was imposed on the controller.

In June, several telecom operators were ordered by the Portuguese SA to delete all the traffic and location data of its users. Such data had been stored for a year by the controllers in specific databases to help law enforcement authorities in their work of

investigating serious crimes. However, the SA argued that the processing of such data under Art. 4 of Law 32/2008 no longer enjoyed a legal basis and therefore, conflicted with the principle of lawfulness of Art. 5(1) (a) GDPR. Indeed, as a result of the Ruling 268/2022 in 2014, key provisions of Law 32/2008 (transposing the Data Retention Directive), such as Art. 4, were found unconstitutional.

## 6.2.1.21. ROMANIA

At the beginning of April, following an investigation of a personal data security breach consisting of the disclosure of the data of 32 employees, the Romanian SA sanctioned a controller with a corrective measure. It was discovered by the SA that the controller had infringed Art. 32(1)(b) and (2) GDPR, which led to the unauthorised disclosure through e-mail of a document containing the employees' personal data.

In May, the Romanian SA issued a fine of EUR 3,000 to the controller Wine Point SRL for violating Art. 32 GDPR by failing to take sufficient technical and organisational measures in order to ensure the confidentiality of the personal data processed. Indeed, the controller sent an e-mail to several individuals at the same time, thereby disclosing their e-mail addresses to everyone.

The same month, a courier company was sanctioned with a reprimand and a corrective measure by the Romanian SA. This sanction was issued as a result of the processor's breach of Art.32(1)(b), (2) and (4) GDPR.

In July, the cosmetic company Sephora Cosmetics Romania SA was sanctioned with a fine of EUR 2,000 for the breach of Art. 21 GDPR. The Romanian SA established that Sephora dismissed a request from the complainant not to use her personal data for marketing purposes. Indeed, after promising the complainant that her data would not be used, the controller still sent her unsolicited commercial messages.

In early September, the Romanian SA sanctioned a public institution for posting on its website 582 Excel files containing personal data of numerous individuals. It was established that the password for accessing the files had been disclosed, thereby increasing the risk of unauthorised access to the data. A reprimand, as well as a corrective measure, was issued by the SA on the institution for infringing Art. 32(1)(b) and (2) GDPR.

Later in September, the Romanian SA reprimanded the controller Târgu-Jiu Emergency County Hospital for infringing Art. 5(1)(a), (c) and (2) in conjunction with Art. 6 GDPR. The controller had published the complainant's personal data on the Internet without his consent and failed to answer the complainant's request. The complainant had asked to receive information regarding the personal data security policy as well as the reasons and the legal basis for disclosing his data. In addition to the fine, the SA ordered the controller to ensure that his processing operations complied with the GDPR and that the persons processing data under his authority be trained.

In October, a commercial company was sanctioned by the Romanian SA for collecting and disclosing on its website the personal data of natural persons and former employees of some companies without their consent. The controller was sanctioned with:

- a fine of EUR 5,000 for infringing Art.6(1) in conjunction with Art. 5(1)(a) GDPR;
- a reprimand for the breach of Art. 5(1)(d) GDPR; and
- a reprimand for the breach of Art. 14 corroborated with Art. 12 GDPR.

## 6.2.1.22. SLOVENIA

In 2022, the Slovenian SA handled several cases. A few cases of particular importance are presented in this section.

In July, the Slovenian police was ordered by the SA to reconsider a specific case as it did not determine all the substantial circumstances and facts. The case concerned an individual's request to access personal data (Art. 15 GDPR) regarding her entry in the Republic of Slovenia, through a particular border crossing point. The request was rejected by the controller for the reason that it did not keep a record of crossings at the national border. The complainant responded to the police's decision by filing an appeal.

In early October, the Slovenian SA ordered a controller to stop processing the location data of employees using its delivery vehicles. The SA found that the data was continuously, systematically and automatically processed by the controller through GPS tracking which enabled him to immediately determine who was using the company vehicle and where the employee was located. The SA concluded that the tracking was disproportionate to the aim pursued (i.e. safety of individuals in case of traffic incidents), there was no legal basis of legitimate interests for processing (Art. 6(1)(f) GDPR) and the GPS tracking infringed the principle of data minimisation (Art. 5(1)(c) GDPR).

Later in the month, an employer in the private sector was ordered by the Slovenian SA to remove its cameras monitoring work areas as it failed to fulfil the requirement of necessity. Indeed, the SA argued that other milder measures could have been used to monitor the compliance of work tasks (i.e. the use of machinery) with working safety rules, such as employees' statements or by using the data processed by the machinery itself.

In September, the Slovenian SA handled a case concerning a request made by an individual to receive the documents and information about the recipients of his data. In this case, the SA concluded that the documentation the complainant had asked to access, enclosed information about the market performance of an economic entity and not data of a natural person. Hence, the SA argued that there was no legal basis for

the individual to receive the documents, nor the list of recipients of the data.

In December, a warning was issued by the Slovenian SA to a public penal institution for failing to put in place technical and organisational measures ensuring that video recordings would not be deleted. This warning was issued after an applicant had requested a copy of a video recording capturing his movements in a particular area of the prison during a specific date and was denied access to the data. It was established by the SA that the recording video had been automatically deleted by the controller after the request of the complainant had been submitted.

#### **6.2.1.23. SPAIN**

In 2021, the Spanish SA dealt with five cases involving the issuance of duplicate SIM cards to third parties other than subscribers. In those cases, the Spanish SA issued hefty fines for the violation of Art. 5(1)(f) GDPR. In separate decisions, the controllers Telefónica Móviles España, Orange Espagne, Xfera Móviles and Orange España Virtual were accused of failing to implement appropriate measures, thereby generating the loss of confidentiality and the transfer of personal data to a third party. The largest fine (EUR 3,940,000) was imposed on the controller Vodafone Espanã as not only did the company infringe Art. 5(1)(f) GDPR, but it also violated the principle of accountability under Art. 5(2) GDPR.

Furthermore, in March 2022, the Spanish SA imposed a fine of EUR 10,000,000 on the controller Google LLC for two infringements of the GDPR, namely lawfulness of processing (Art. 6) and the right to erasure (Art. 7). The Spanish SA found that the controller was transferring data without legitimacy to Lumen Database and was obstructing the right of erasure.

In 2022, the Spanish SA dealt with two cases concerning the processing of personal data on pornographic websites. The possibility that minors could register on the website and have direct,

uncontrolled access to pornographic content was a major problem in these cases. Upon registering, the minors' data was processed by the controllers. The Spanish SA ordered the controllers Burwebs S.L and Techpump Solutions S.L to implement, within a month, the necessary corrective measures to ensure that their activities complied with data protection regulations and that minors were effectively prevented from having access to the website's content. Additionally, the Spanish SA issued Burwebs a fine of EUR 75,000 for the infringement of Arts. 5(1)(a), (b) and (e), 8, 12(2), 13, 25 and 30 GDPR and Art. 22(2) of the Law of Information Society Services and Electronic Commerce (LSSI). On the other hand, Techpump Solutions was issued a fine of EUR 525,000 for the violations of Arts. 5(1)(a), (b) and (e), 6(1), 8, 12(1), 12(2), 13, 25 and 30 GDPR and Art. 22(2) LSSI.

#### **6.2.1.24. SWEDEN**

In this section, three enforcement measures conducted in 2022 by the Swedish SA for violations of the GDPR will be presented.

On 14 March, the Swedish Customs was issued an administrative fine of EUR 30,000 by the SA. It was established that the controller had not taken the necessary technical and organizational measures to prevent the data breach. Indeed, the technical barriers which had been set by the controller to restrict the storage and copying of data from staff mobiles in a US cloud service were not strong enough.

Later in the month, a financial company named Klarna was issued a fine of EUR 700,000 for numerous infringements of the GDPR. This includes the failure to provide information on the purpose and legal basis of the processing of personal data as well as to disclose to which non-EU countries the data was transferred to. Additionally, the Swedish SA discovered during its investigation that the controller has provided incomplete information about the data subject's rights.

The Swedish SA issued two separate fines in 2022 on different controllers within the same case, for breaching Art. 32 GDPR. In other words, both the Regional Board and the Hospital Board within the Region of Uppsala were condemned by the Swedish SA for failing to adequately secure the processing of sensitive data. The Regional Board was imposed an administrative sanction of EUR 30,000 as the information contained in the emails it had distributed to healthcare administrations within the region was not encrypted, thereby opening the door to unauthorised access. On the other hand, the Hospital Board was issued a fine of EUR 160,000, as not only did it fail to implement adequate security measures, but it also processed the data of patients in breach of Art. 5(1)(f) GDPR.

### **6.3. SA SURVEY - BUDGET AND STAFF**

Statistics on resources made available by Member States to the SAs from the EEA are gathered by the EDPB each year. On 5 September 2022, the EDPB published an “[Overview on resources made available by Member States to the Data Protection Supervisory Authorities](#)”. Most SAs (23) explicitly stated that their allocated budget is not sufficient for carrying out their activities, while some SAs considered they had sufficient financial resources. Based on information provided by 30 SAs from EEA countries prior to September 2022, five SAs saw budgetary decreases in contrast to their 2021 budget.

Eight SAs faced a decrease in employees compared to 2021. Overall, a vast majority of SAs (26) underlined that they do not have enough human resources to face their workload.

In its [Contribution to the evaluation of the GDPR under Art. 97](#) adopted in 2020, the EDPB underlined that the SAs' ability to carry out their duties attributed by the GDPR is largely dependent on the resources made available to them.

# 7

## COORDINATED SUPERVISION COMMITTEE OF THE LARGE EU INFORMATION SYSTEMS AND OF EU BODIES, OFFICES AND AGENCIES

As reflected in Art. 62 of Regulation 2018/1725, an active collaboration between the European Data Protection Supervisor (EDPS) and national Supervisory Authorities (SAs) is required to ensure the effective supervision of large-scale IT systems and of EU bodies, offices and agencies. While in the past the EDPS and the involved SAs cooperated through a system of individual Supervision Coordination Groups (SCGs),<sup>55</sup> in December 2019, the Coordinated Supervision Committee (CSC) was established within the EDPB to ensure the consistency of supervision efforts on all levels.

The CSC brings together the SAs of each EU Member State and the EDPS, as well as SAs of non-EU Members of the Schengen Area when foreseen under EU law. In the period between 2020-2022, the CSC carried out numerous notable tasks: it promoted and facilitated

the exercise of data subject rights, examined the interpretation or application issues concerning EU and national law, exchanged relevant information, conducted joint audits and inspections, as well as prepared for the start of the activities of the European Public Prosecutor Office and other EU bodies and information systems falling under the Committee's scope.

Participation in the CSC meetings can occur under various arrangements, depending on the IT system, body, office or agency for which supervision is taking place, as well as the respective EU legal act.

Pursuant to Art. 62 of Regulation 2018/1725, the following EU large-scale IT systems, bodies, offices and agencies currently fall under the CSC's scope:

<sup>55</sup> In the past, four SCGs were created for the following systems: Schengen, Visa and Customs Information Systems, as well as for Eurodac.

## **Internal Market:**

- Internal Market Information System (IMI), which allows the exchange of information between public authorities involved in the practical implementation of EU law.

## **Police and Judicial Cooperation:**

- Eurojust, the agency responsible for judicial cooperation in criminal matters among EU Member States;
- European Public Prosecutor Office (EPPO), the prosecution agency responsible for investigating, prosecuting and bringing to judgment crimes against the EU budget;
- European Union Agency for Law Enforcement Cooperation (Europol).

In the future, all coordinated supervision of large EU information systems, bodies, offices and agencies will gradually be moved to the CSC, including:

## **Border, Asylum and Migration:**

- Schengen Information System (SIS), ensuring border control cooperation;
- Entry Exit System (EES), which registers entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Schengen States ;
- European Travel Information and Authorisation System (ETIAS), which tracks visitors from countries who do not need a visa to enter the Schengen;
- Visa Information System (VIS), connecting consulates in non-EU countries and all external border-crossing points of Schengen States;

- Eurodac, which compares fingerprints of asylum applicants to see if they have previously applied for asylum or entered the EU irregularly via another Member State;
- Customs Information System (CIS), which is an automated information system that assists EU State administrative authorities in preventing, investigating and prosecuting operations that are in breach of customs or agricultural legislation.

## **Police and Judicial Cooperation:**

- European Criminal Records Information System on third country nationals (ECRIS-TCN), which allows EU Member State authorities to identify which other Member States hold criminal records on third country nationals or stateless persons being checked ;
- Schengen Information System (SIS) (see above, as this system also fall under Police and Judicial cooperation).

More relevant info can be found in the EDPB's [bi-annual report on the CSC](#).

# 8

## ANNEXES

### 8.1. GENERAL GUIDANCE ADOPTED IN 2022

- Guidelines 01/2021 on Examples regarding Personal Data Breach Notification
- Guidelines 04/2021 on Codes of Conduct as tools for transfers (version 2.0)
- Guidelines 01/2022 on data subject rights - Right of access
- Guidelines 02/2022 on the application of Article 60 GDPR
- Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them
- Guidelines 04/2022 on the calculation of administrative fines under the GDPR
- Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement
- Guidelines 06/2022 on the practical implementation of amicable settlements
- Guidelines 07/2022 on certification as a tool for transfers
- Guidelines 8/2022 on identifying a controller or processor's lead supervisory authority
- Guidelines 9/2022 on personal data breach notification under GDPR

- Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR)

### 8.2. CONSISTENCY OPINIONS AND DECISIONS ADOPTED IN 2022

- Decision 01/2022 on the draft decision of the French Supervisory Authority regarding Accor SA under Article 65(1)(a) GDPR
- Binding Decision 2/2022 on the draft decision of the Irish Supervisory Authority regarding Meta Platforms Ireland Limited (Instagram) under Article 65(1)(a) GDPR
- Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR)
- Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65 GDPR)
- Binding Decision 5/2022 on the dispute submitted by the Irish SA regarding WhatsApp Ireland Limited (Art. 65 GDPR)
- Opinion 1/2022 on the draft decision of the Luxembourg Supervisory Authority regarding the GDPR – CARPA certification criteria
- Opinion 02/2022 on the draft decision of the French Supervisory Authority regarding the

Controller Binding Corporate Rules of the WEBHELP Group

- Opinion 03/2022 on the draft decision of the French Supervisory Authority regarding the Processor Binding Corporate Rules of the WEBHELP Group
- Opinion 04/2022 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of Norican Group
- Opinion 05/2022 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of the Lundbeck Group
- Opinion 06/2022 on the draft decision of the Irish Supervisory Authority regarding the Controller Binding Corporate Rules of Groupon International Limited
- Opinion 07/2022 on the draft decision of the Hungarian Supervisory Authority regarding the Controller Binding Corporate Rules of MOL Group
- Opinion 08/2022 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of Bioclinica Group
- Opinion 09/2022 on the draft decision of the Danish Supervisory Authority regarding the Processor Binding Corporate Rules of Bioclinica Group
- Opinion 10/2022 on the draft decision of the Hesse Supervisory Authority (Germany) regarding the Controller Binding Corporate Rules of Fresenius Group
- Opinion 11/2022 on the draft decision of the competent supervisory authority of Poland regarding the approval of the requirements for

accreditation of a certification body pursuant to Article 43.3 (GDPR)

- Opinion 12/2022 on the draft decision of the competent supervisory authority of France regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)
- Opinion 13/2022 on the draft decision of the competent supervisory authority of Bulgaria regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)
- Opinion 14/2022 on the draft decision of the competent supervisory authority of Bulgaria regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR
- Opinion 15/2022 on the draft decision of the competent supervisory authority of Luxembourg regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR
- Opinion 16/2022 on the draft decision of the competent supervisory authority of Slovenia regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR
- Opinion 17/2022 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of the ANTOLIN Group
- Opinion 18/2022 on the draft decision of the Baden- Württemberg (Germany) Supervisory Authority regarding the Controller Binding Corporate Rules of the Daimler Truck Group
- Opinion 19/2022 on the draft decision of the Baden- Württemberg (Germany) Supervisory

- Authority regarding the Controller Binding Corporate Rules of the Mercedes-Benz Group
- Opinion 20/2022 on the draft decision of the Irish Supervisory Authority regarding the Controller Binding Corporate Rules of the Ellucian Group
- Opinion 21/2022 on the draft decision of the Irish Supervisory Authority regarding the Processor Binding Corporate Rules of the Ellucian Group
- Opinion 22/2022 on the draft decision of the Liechtenstein Supervisory Authority regarding the Controller Binding Corporate Rules of the Hilti Group
- Opinion 23/2022 on the draft decision of the Swedish Supervisory Authority regarding the Controller Binding Corporate Rules of the Samres Group
- Opinion 24/2022 on the draft decision of the Swedish Supervisory Authority regarding the Processor Binding Corporate Rules of the Samres Group
- Opinion 25/2022 regarding the European Privacy Seal (EuroPriSe) certification criteria for the certification of processing operations by processors
- Opinion 26/2022 on the draft decision of the Data Protection Authority of Bavaria for the Private Sector regarding the Controller Binding Corporate Rules of the Munich Re Reinsurance Group
- Opinion 27/2022 on the draft decision of the French Supervisory Authority regarding the Processor Binding Corporate Rules of LEYTON Group
- 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)
- Opinion 29/2022 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of the DSV Group
- Opinion 30/2022 on the draft decision of the Slovak Supervisory Authority regarding the Controller Binding Corporate Rules of Piano Group
- Opinion 31/2022 on the draft decision of the Slovak Supervisory Authority regarding the Processor Binding Corporate Rules of Piano Group
- Opinion 32/2022 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of the Ramboll Group

## 8.3. JOINT OPINIONS ADOPTED IN 2022

- EDPB-EDPS Joint Opinion 1/2022 on the extension of the Covid-19 certificate Regulation
- EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)
- EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space
- EDPB-EDPS Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse

## 8.4. LEGISLATIVE CONSULTATION

- Statement 01/2022 on the announcement of an agreement in principle on a new Trans-Atlantic Data Privacy Framework

- Statement 04/2022 on the design choices for a digital euro from the privacy and data protection perspective
- Statement on the implications of the CJEU judgment C-817/19 on the use of PNR in Member States
- EDPB Letter to the EU Commission on procedural aspects that could be harmonised at EU level
- Response of the EDPB to the European Commission's targeted consultation on a digital euro

## 8.5. OTHER DOCUMENTS

- Statement 02/2022 on personal data transfers to the Russian Federation
- Statement 03/2022 on the European Police Cooperation Code
- Statement on enforcement cooperation ('Vienna statement')
- EDPB Document on selection of cases of strategic importance

## 8.6. LIST OF EXPERT SUBGROUPS AND TASKFORCES WITH SCOPE OF MANDATES

NAME OF EXPERT SUBGROUP (ESG)	SCOPE OF MANDATE
<b>Borders, Travel &amp; Law Enforcement Expert Subgroup (BTLE)</b>	<ul style="list-style-type: none"> <li>• Law Enforcement Directive</li> <li>• Cross-border requests for e-evidence</li> <li>• Adequacy decisions under the Law Enforcement Directive, access to transferred data by law enforcement and national intelligence authorities in third countries</li> <li>• Passenger Name Records (PNR)</li> <li>• Border controls</li> </ul>
<b>Compliance, e-Government and Health Expert Subgroup (CEH)</b>	<ul style="list-style-type: none"> <li>• Codes of conduct, certification and accreditation</li> <li>• Compliance with public law and eGovernment</li> <li>• Processing of personal data concerning health</li> <li>• Processing of personal data for scientific research purposes</li> <li>• Consultation on several legislative proposals by the European Commission within the Digital Strategy</li> <li>• Close cooperation on DPIA with the Technology ESG focusing on the perspective of their mandates</li> <li>• Close cooperation on privacy by design and by default with the Technology ESG focusing on the perspective of their mandates</li> </ul>
<b>Cooperation Expert Subgroup (COOP)</b>	<ul style="list-style-type: none"> <li>• General focus on procedures established by the GDPR for the purposes of the cooperation mechanism</li> <li>• Guidance on procedural questions linked to the cooperation mechanism</li> <li>• International mutual assistance and other cooperation tools to enforce the legislation for the protection of personal data outside the EU (Art. 50 GDPR)</li> </ul>
<b>Coordinators Expert Subgroup (COORD)</b>	<ul style="list-style-type: none"> <li>• General coordination between the Expert Subgroup Coordinators</li> <li>• Coordination on the annual Expert Subgroup working plan</li> </ul>

<b>Enforcement Expert Subgroup (ENF)</b>	<ul style="list-style-type: none"> <li>• Mapping/analysing the need for additional clarifications or guidance, based on practical experiences with the application of Chapters VI, VII and VIII GDPR</li> <li>• Mapping/analysing possible updates of existing Cooperation subgroup tools</li> <li>• Monitoring of investigation activities</li> <li>• Practical questions on investigations</li> <li>• Guidance on the practical application of Chapter VII GDPR including exchanges on concrete cases</li> <li>• Guidance on the application of Chapter VIII GDPR together with the Taskforce on Administrative Fines</li> <li>• Art. 65 and Art. 66 procedures</li> </ul>
<b>Financial Matters Expert Subgroup (FMESG)</b>	Application of data protection principles in the financial sector (e.g. automatic exchange of personal data for tax purposes; impact of FATCA on the protection of personal data; interplay between Second Payment Services Directive and GDPR)
<b>International Transfers Expert Subgroup (ITS)</b>	<p>Guidance on Chapter V (International transfer tools and policy issues), more specifically:</p> <ul style="list-style-type: none"> <li>• Review European Commission Adequacy decisions</li> <li>• Guidelines on Art. 46 GDPR and review of administrative arrangements between public authorities and bodies</li> <li>• Codes of conduct and certification as transfer tools</li> <li>• Art. 48 GDPR together with BTLE ESG</li> <li>• Art. 50 GDPR together with Cooperation ESG</li> <li>• Guidelines on territorial scope and the interplay with Chapter V of the GDPR – interaction with Key Provisions ESG</li> <li>• Exchange of information on review of BCRs and ad hoc contractual clauses according to Art. 64 GDPR</li> </ul>

<b>IT Users Expert Subgroup (IT-Users)</b>	Developing and testing IT tools used by the EDPB with a practical focus: <ul style="list-style-type: none"> <li>• Collecting feedback on the IT system from users</li> <li>• Adapting the systems and manuals</li> <li>• Discussing other business needs including tele- and videoconference systems</li> </ul>
<b>Key Provisions Expert Subgroup (KEYPROV)</b>	Guidance on core concepts and principles of the GDPR, including Chapters I (e.g. scope, definitions like LSA and large-scale processing) and II (main principles); Chapters III (e.g. rights of individuals, transparency), IV (e.g. DPO – shared competences with CEH ESG, Enforcement ESG and Technology ESG) and IX
<b>Social Media Expert Subgroup (SOCM)</b>	<ul style="list-style-type: none"> <li>• Analysing social media services, conceived as online platforms that focus on enabling the development of networks and communities of users, among which information and content is shared and whereby additional functions provided by social media services include targeting, personalisation, application integration, social plug-ins, user authentication, analytics and publishing</li> <li>• Analysing established and emerging functions offered by social media, including the underlying processing activities and corresponding risks for the rights and freedoms of individuals</li> <li>• Developing guidance, recommendations and best practices in relation to both the offer and use of social media functions, in particular for economic or political reasons</li> <li>• Providing assistance to other subgroups, in particular by proposing strategic priorities in terms of (a) supervision and (b) the development of new EDPB guidance or updating of existing WP29 guidance</li> </ul>
<b>Strategic Advisory Expert Subgroup (SAESG)</b>	<ul style="list-style-type: none"> <li>• Guidance on strategic questions affecting the whole EDPB (including the discussion on the strategy and on the work plans of the ESGs)</li> <li>• Clarification of questions that could not be resolved in the ESG</li> </ul>
<b>Taskforce on Administrative Fines (Fining-TF)</b>	Development of Guidelines on the harmonisation of the calculation of fines

<b>Technology Expert Subgroup (TECH)</b>	<ul style="list-style-type: none"><li>• Technology, innovation, information security, confidentiality of communication in general</li><li>• ePrivacy, encryption</li><li>• DPIA and data breach notifications</li><li>• Emerging technologies, innovation and other challenges related to privacy: reflecting on data protection risks of future technological developments</li><li>• Providing input on technology matters relevant to other ESG</li></ul>
--	---

## CONTACT DETAILS

Postal address  
Rue Wiertz 60, B-1047 Brussels

Office address  
Rue Montoyer 30, B-1000 Brussels